N-CENTRAL 6

Customer Manual

Version 6.0

N-able

MONITOR • MANAGE • OPTIMIZE®

www.n-able.com

info@n-able.com

1-877-655-4689

Contents

Preface

About this Manual

This manual describes the services in N-central® and the details of each service that can be set to monitor the devices of a network.

Audience

This manual is intended for all of the users of N-central who set up the services to be monitored on a device or view the status of the monitored devices.

The use of N-central requires familiarity in the following areas of technology:

- client-server architecture and agents; and
- Transmission Control Protocol/Internet Protocol (TCP/IP) networks, including firewall theory, proxy theory, network address translation, routing tables, the Simple Mail Transfer Protocol (SMTP), and Public Key Infrastructure (PKI) theory.

Conventions

Following are the document conventions used in this manual.

Convention	Use
Permission Level:	Indicates the permission level required for the feature described in the subsequent section to be available.
blue	Indicates a hyperlink.
`Courier`	Indicates text in a script or terminal window.
italics	Indicates a book title or reference document.
Sans Serif	Indicates the items in the user interface, including screen titles, menus, fields, and buttons.
↳	Indicates the expected behavior of the tool upon completing an action.
>	Indicates a menu selection. For example, “Select File>Open”.
< >	Encloses a variable.
[ ]	Encloses an optional parameter.

What's New?

This section provides a brief summary of new functionality in N-central 6.0 and the changes to existing functionality from the previous release. Following each summary are cross-references to more detailed sections in the manual.

Features

The following capabilities have been added or revised in N-central 6.0:

Agent-Based Automatic Workstation Disconnection

N-central now provides for the automatic disconnection of agent-monitored workstations if the workstation shuts down or does not communicate with the central server within a specified time frame. For more information, please refer to the *Customer Manual.*

Removal of System Notifications for Stale Agents or Probes

N-central no longer sends system stale notifications when the agent or probe is in a stale state after a specified length of time.

Intel® vPro™

N-central now provides the functionality for you to remotely turn on, off or restart an Intel® vPro™ device. For more information, please refer to the *Customer Manual*.

Patch Management

The patch management feature includes new reports and two new services: MBSA 2.0, which supports version 2.0 of MBSA; and Patch Management, which monitors patch compliance. In addition, the Patch Level service has been updated and renamed MBSA 1.2.1.

For information about patch management services and reports, refer to Services and Reports below.

Remote Support Manager

Remote Support Manager is a powerful desktop management platform that provides increased functionality for managing, supporting, and securing desktops and applications in a Windows-based environment. For more information, please refer to the *SO Customer* and *Customer Manuals*.

Note: Additional information about Remote Support Manager can also be found in the Remote Support Manager documentation in the Partner Resource Centre on the N-able Web site.

Services

The following services have been added or revised in N-central 6.0:

Agent Status

The Agent Status service monitors the amount of time since the agent last checked in with the central server. This service allows the central server to monitor devices that have agents. If this service enters a Failed state, the central server will disconnect other services. For more information, please refer to Agent Status on page 11.

Device Status

The Device Status service monitors the current operational state of a device and reports information such as the device's manufacturer, revision value, and (optionally), the device's serial number. For more information, please refer to Device Status on page 89.

Intel® vPro™ Status

You can monitor the network availability of the Intel® vPro™ interface and the power status of an Intel® vPro™ device through the new service, Intel® vPro™ Status. For more information, please refer to Intel® vPro™ Status on page 155.

Patch Level Service Renamed MBSA 1.2.1

The Patch Level service has been updated and renamed to MBSA 1.2.1. It now supports MBSA 1.2.1. For more information, please refer to MBSA 1.2.1 on page 173.

MBSA 2.0

A new service called MBSA 2.0 has been added to support version 2.0 of MBSA. For more information, please refer to MBSA 2.0 on page 177.

Patch Management

The Patch Management service monitors devices to determine whether or not required updates and patches have been installed. For more information, please refer to Patch Management on page 189.

Probe Status

The Probe Status service monitors the time since the probe last checked in with the central server. This allows the central server to represent the appropriate state of the probe on the status dashboard. For more information, please refer to Probe Status on page 211.

Reports

The following reports have been added or revised in N-central 6.0:

Patch - Non-Compliant Computers By Classification

The Patch - Non-Compliant Computers By Classification report allows you to view a list of updates that have been missed.

Patch - Single Computer Missed Updates

The Patch - Single Computer Missed Updates report provides a summary of all missed updates for a selected device.

Patch - Update Installation Status - Multi-computer

The Patch - Update Installation Status - Multi-computer report displays the number of updates by installation status for each device.

Patch - Update Installation Status - Single Computer

The Patch - Update Installation Status - Single Computer report displays the number of updates by installation status for a specified device.

Patch - Updates Required

The Patch - Updates Required report lists all updates that have been missed by each device.

Patch - WSUS Non-Compliant Devices By Device

The Patch - WSUS Non-Compliant Devices By Device report lists all devices that are missing updates.

Remote Support Manager

The Remote Support Manager report displays the number of devices with Remote Support Manager (RSM) enabled as well as the number of Remote Support Manager clients that have been installed. You can also choose to include the devices without Remote Support Manager enabled, as well.

For more information, please refer to .

Chapter 1

About Services

A service in N-central represents an element (or service) that runs on your device. For example, the CPU service monitors the CPU utilization on a computer and the HTTP service monitors the availability and response time of a Web server application. By monitoring the devices of your network, the services help you quickly locate your network's problem areas and optimize its performance.

The monitored results are interpreted through seven types of states, which are: Normal, Warning, Failed, Misconfigured, No Data, Stale Data, and Disconnected.

The state of a service can be viewed on the status dashboard on which the service appears. For example, the state of the CPU service for a device can be viewed on the Standard Services dashboard. A service changes state based on settings specified on the Service Details and Threshold tabs of the service. These tabs are available only to an N-central administrator.

The monitoring of a service on a device requires:

- adding the device to N-central;
- setting up the monitoring agent or probe according to network specifications;
- adding the representing N-central service on the device; and
- setting up the service by specifying information on the Service Details and Threshold tabs of the service.

Note: Only services that have been enabled by a Product Administrator or SO Admin can be monitored on the status dashboards.

Service Details

Service Details contain settings on the parameters and scan details for services, including regular expression settings for some services.

Table 1-1 describes the service details that are common across two or more services.

Table 1-1: Common Service Details

Service Detail	Description
End Hour	The end hour of a log file scan. The service scans from the specified Start Hour until the end of the specified End Hour at time intervals specified for Scan Interval in Minutes. For example, if you choose 01:00 as the Start Hour, 02:00 as the End Hour, and 30 as the Scan Interval in Minutes, the service will scan at 1:00, 1:30, 2:00, and 2:30. **Note:** The End Hour is the last hour in which the service will scan, not the cut-off time for the scan.
Log File Name and Path	The directory path and name of a log file that you would like monitored by the service. The name and path specified can be complete or partial. For example: c:\test.log,c:*.log, c:\test*
Monitoring	The status of the service: • Enabled, which begins the immediate monitoring of the service on the device. • Disabled, which prevents monitoring of the service on the device. When you would like to temporarily stop the monitoring process, disable the service rather than deleting the service.
Current Monitoring Probe	The central server, probe, or local agent that is being used to monitor the service.
Change Monitoring Probe	The central server, probe, or local agent that is to be used to monitor the service.
Port Number	The TCP port number used to monitor a specific TCP based service.
Regular Expressions 1 to 6	The strings of characters and metacharacters that you would like to use to find predetermined key words in the log file(s). You can set a different threshold option for each regular expression.
Repeat Monthly on Day(s)	The log file scan is repeated monthly on the specified days. If you do not select this option but do select an option for the other scan details, N-central scans continuously.
Repeat Weekly on Day(s)	The log file scan is repeated weekly on the specified days. If you do not select this option but do select an option for the other Scan details, N-central scans continuously.
Scan Interval (Also appears only for scheduled scans)	The time (in minutes) between each scan.
Service Description	A description of the service.
Start Hour	The start hour of a log file scan. The service starts scanning at the specified Start Hour and continues scanning until the end of the End Hour at time intervals specified for Scan Interval in Minutes. For example, if you choose 01:00 as the Start Hour, 02:00 as the End Hour, and 30 as the Scan Interval in Minutes, the service will scan at 1:00, 1:30, 2:00, and 2:30.

Service Detail	Description
Time Offset	The age of a log file (in hours). When the agent scans the log file, it compares the time at which the log file was last updated with its current time scan. If the difference is greater than the specified time offset, the agent reports the Failed state for the service. Otherwise the agent reports the Normal state. If you are using Veritas to backup your database once a day, we recommend that you set the time offset to 23 (hours).
Time to Stale	The time (in minutes) for the most recent monitored data to become stale. The value must be greater than or equal to the Scan Interval value. Otherwise, the service will be constantly in the Stale state.
Timeout Value	The time (in seconds) that the central server waits before considering the test a failure.
Validating String	A regular expression that determines whether the response sent by the queried device is valid.

Thresholds

Thresholds contain editable settings on scan details that trigger state changes for a service. A service changes state when it crosses a threshold.

N-central uses the threshold information to determine the state of a service based on the raw monitored data. To determine the state of a service, N-central compares the raw data gathered during monitoring against specified thresholds.

States

You can configure threshold values for the following states:

- Normal,
- Warning, and
- Failed.

If N-central cannot set the threshold to Normal, Warning, or Failed, then it will set the threshold to the Indeterminate state. The Indeterminate state is then displayed as Misconfigured or No Data on the status dashboard.

The Indeterminate state displays as Misconfigured if:

- errors are returned by the agent,

  For example, the agent returns error messages, such as `102 could not open the system event log` to the central server.

- values are missed during threshold configuration, and

  For example, threshold ranges for Normal (0-50), Warning (45-85), and Failed (87-100) are specified for a service and the agent returns the value 86, which has not been included in a range.

- proper parameters have not been specified.

  For example, if the Disk service was added on a device but not set up with the name of the volume that needs to be monitored.

The Indeterminate state displays as No Data if the central server does not receive data from the agent.

Monitoring Options

Following are the four monitoring options that are supported in N-central:

- Normal, which changes the service to Failed when the service stops running.
- Reversed, which inverts the monitoring process. For example, a process that should not be running on a device can be monitored by the Process service using this method. Once the process starts running, the state for the Process service changes to Failed.
- Custom, which allows you to set up values for the Normal, Warning, and Failed states. For example, threshold settings for scan details, such as file size, average round trip time, and time to live (TTL) can be customized.
- Off, which stops processing the scan detail for a state. If one scan detail is set to Off, the service is processed for a state based on the thresholds of the rest of the scan details. If all of the scan details are set to Off, the service is processed for its availability.

Regular Expressions

Regular expressions contain strings of characters and metacharacters specified by the user to find predetermined key words in a log file. Metacharacters are symbols that take the form of grammatical punctuation, numbers, and the alphabet. In N-central, metacharacters are used with character strings to increase the probability of finding keywords in a specified log file. Regular expressions are specified in the Service Details tab for some of the N-central services. The parameters for the regular expressions are specified in the Thresholds tabs of these services.

Table 1-2 describes the basic regular expressions that can be used.

Table 1-2: Basic Regular Expressions

Metacharacter	Match	Example
.	Matches any single character except newline.	b.t Scans for the line containing a **b** followed by any character and a **t**.
*	Matches an expression that has 0 or more of the preceding character.	bt* Scans for the line containing a **b** followed by 1 or more **t**'s.
+	Matches an expression that has one or more of the preceding character.	bt+ Scans for the line containing a **b** followed by at least one **t**.
^	Matches the beginning of a line.	^bt Scans for the line that begins with **bt**.
$	Matches the end of a line.	bt$ Scans for the line that ends with **bt**.

Metacharacter	Match	Example
\ (The escape character)	Prevents the function of the subsequent metacharacter.	file1\.dll Scans for the line containing file1.dll. To allow the “period” to be a part of the line, the “\” prevents the “period” from functioning as a metacharacter.
[ ]	Matches any character that is within these brackets.	[Bb]t[0-9] Scans for the line that contains an upper or lowercase **b**, a lowercase **t**, followed by a digit that is between and including zero and nine.
?	Matches an expression that has 0 or 1 of the proceeding character.	bt? Scans for the line that contains a **b** that may or may not be followed by a **t**.

Service Types

The following types of services are monitored in N-central:

- System services,
- Network services,
- Security services, and
- VoIP.

Table 1-3 lists the service types and their method of collecting data during the monitoring process.

Table 1-3: Service Types and Collection Methods

Service Type	Collection Method
System	Local API, Remote WMI, or SNMP
Network	SNMP or TCP
Security	Local API, Remote WMI, or Syslog
WSUS	N-able Connector
VoIP	SNMP or Remote WMI

The service types are monitored by agents and probes. Agents are used when the central server can route to the devices. Probes are used when the central server cannot route to devices, especially if the devices are behind a firewall. Local APIs, WMI, SNMP, TCP, and syslog protocols are used by the agents and probes during the monitoring process.

Table 1-4 indicates which agent or probe can be used to monitor a particular service type.

Table 1-4: Monitoring of Service Types

Monitoring Agent/Probe	System			Network		Security			VoIP	
	Local API	Remote WMI	SNMP	SNMP	TCP	Local API	Remote WMI	Syslog	SNMP	Remote WMI
Agent	x	x	x			x				
Central Server					x	x				
Central Server Asset		x*								
Network Hardware Probe				x	x	x		x	x	x
Network Windows Probe**		x		x	x	x	x	x	x	x
Workgroup Windows Probe**		x		x	x	x	x	x	x	x
WSP		x			x	x	x		x	x

**The Central Server Asset can only monitor the System Change, System Check-In, System Replacement, and System Warranty services.*

The Network Windows Probe and Workgroup Windows Probe can only monitor Remote WMI services if the probe is installed with domain administrator privileges* ***or *if the monitored device is within the same workgroup and has the same username and password as the probe.*

System Services

System services can be monitored locally or remotely.

Local System Services

Local system services are monitored using agents. Agents can monitor operating systems, such as Windows, Novell, Mac, RedHat Linux, Sun Solaris, and SUSE Linux. The agents are installed locally on each monitored device. They must be installed immediately after setting the local system services on a device, otherwise, the states of the local services will change from the No Data state to Stale Data state. Once installed, the agents use Application Program Interfaces (APIs) and system and log files that are available on the operating system to obtain information on the local services of the device.

Remote WMI

Remote system services are Windows-based services and monitored using the Windows probes. The Windows probes use the Windows Management Instrumentation (WMI) protocol to obtain information on the local services of a device. Information can only be obtained if the probe is:

- installed within the same domain as the monitored devices;
- set up with domain administrator privileges; and

- the WMI option is selected on the devices. For Windows 2000, XP, and 2003, this protocol is selected by default.

Network Services

Network services are monitored using probes, which run network-based tests on the service availability, round trip time, and Domain Name System (DNS) resolution to determine the service performance. The tests are run using protocols, such as the Simple Network Management Protocol (SNMP), Transmission Control Protocol (TCP), Internet Protocol (IP), Internet Control Message Protocol (ICMP), and Windows Management Instrumentation (WMI).

During a test, the probe makes a TCP port call to a specific port on a target device and waits for the device to respond. The probe then compares the round trip time of the request and response to a specified threshold and displays the appropriate state for the service.

SNMP Services

SNMP-based services are monitored using a set of SNMP management information base (MIB) objects. These services can be used to monitor the performance of the underlying network infrastructure.

Security Services

Security services monitor events that are generated by two main sources: security appliances and security applications.

Security Appliances

Security appliances, such as firewalls, are special-purpose devices with integrated software and hardware that allows them to accomplish their objectives. Security appliances are monitored only after they are:

- added to N-central as devices, and
- configured to send their security events to a probe.

During a test, the probe records and processes the security events from syslog messages. The data is then sent to the central server to be interpreted under the appropriate state for the service.

Security Applications

A security applications, such as anti-virus software, reside on computers and record occurring events in locally saved log files. Security applications are monitored only after their devices are:

- added to N-central, and
- configured to use a Network Hardware Probe, Windows probe, or agent software.

During a test, the Windows probe or agent records and processes the events logged by the device’s security applications. The data is then sent to the central server to be interpreted under the appropriate state for the service.

VoIP Services

VoIP services monitor the VoIP devices, lines, and gateways that are connected to the Cisco CallManager (CCM) application. The services can monitor the presence of the devices on the VoIP network, the availability of the CCM application, its resources—such as Music on Hold, transcoders—and conference hardware, and the server itself on which the CCM application is installed.

The VoIP services use Network Hardware, Network Windows, and Windows Workgroup probes to monitor the VoIP devices.

Chapter 2

Active Directory

Service Type: System

Collection Method: WMI Server

Instances on a Device: Multiple

Supported Platforms: Windows 2000 and Windows 2003 Domain Controllers

Device Class: Windows Server

Monitored By: Windows Probes

Service Version: N-central 5.0 and greater

Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* published by Microsoft®.

The Active Directory service monitors the performance of the Active Directory LDAP service.

Service Details

Active Directory Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	

Status Details

Active Directory Status Details

Status Detail	Description
Bind Time (ms)	Time (in milliseconds) taken for the last successful LDAP bind.
Successful Binds	Number of LDAP binds since last reboot.
Writes	The rate at which LDAP clients perform write operations, per second.
UDP Operations	The number of UDP operations the LDAP server is processing.
Active Threads	The current number of threads in use by the LDAP subsystem of the local directory service.
Client Sessions	The number of connected LDAP client sessions.
Inbound Updates in Packet	The number of object updates received in the current directory replication updates packets that have not yet been applied to the local server. This counter tells you if the monitored server is receiving changes, and is taking too long to apply them to the database.
Pending Replication Syncs	The number of directory synchronizations that are in queue for this server. This counter identifies replication backlog—the larger the number, the larger the backlog.

Chapter 3

Agent Status

Service Type:	System
Collection Method:	Central Server Asset
Instances on a Device:	Single
Supported Platforms:	All available agents
Device Class:	Generic Server, Generic Workstation, Windows Server, and Windows Workstation
Monitored By:	Central Server Asset
Service Version:	N-central 6.0 and greater

The Agent Status service monitors the time since the agent last checked in.

This service only monitors devices that have an agent. In addition, the Agent Status service will automatically begin monitoring the device when an agent is installed.

When Agent Status is first added to a device, the service will be in a Misconfigured state until the agent first makes contact with the central server.

During the monitoring process, the central server queries the time of the most recent connection of a device's agent to the network. This is compared to the current time and the resulting difference is then compared to the specified threshold values so that it can be represented by the appropriate state on the status dashboard for the service.

Example: If the time difference between the previous and current connection is within 10 minutes, the service state will display Normal; between 10 and 20 minutes, Warning; and over 20 minutes, Failed.

If this service enters a Failed state, the central server will disconnect all other services with the exception of the following:

- Intel® vPro™ Status,
- System Change,
- System Check-In,
- System Replacement, and
- Warranty Expiry.

To prevent services from being disconnected, ensure that the Unscheduled Downtime checkbox on the Add Device screen (or in the Details tab of the Edit Device screen) is not selected.

Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	

Status Details

Status Detail	Description
Check-In Interval	The threshold that compares the time difference between the current time and the most recent connection to the specified threshold values.

Chapter 4

AV - Security Center

The AV - Security Center service provides consolidated management of antivirus applications. The service reports the following information for antivirus software:

- product name,
- scanning status,
- current status of updates, and
- version information.

Service Type:	Security
Collection Method:	WMI
Instances on a Device:	Single
Supported Platforms:	Windows XP, Windows Vista
Device Class:	Windows Server, Windows Workstation
Monitored By:	Windows Probe, Windows Agent
Service Version:	N-central 6.0 and greater

The AV - Security Center service supports the following antivirus applications:

- AVG© 7.5
- CA© AntiVirus 2007
- Kaspersky® Anti-Virus 6.0
- McAfee® VirusScan® Enterprise v8.5
- McAfee® Total Protection for Small Business
- Norton AntiVirus™ 2007
- Panda™ WebAdmin AntiVirus
- Symantec AntiVirus™ Corporate Edition 10.0
- Trend Micro™ Anti-Virus 2007

Service Details

AV - Security Center

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	120 minutes

Service Detail	Description
Service Description	This service uses the root\SecurityCenter WMI class on a Windows XP/Vista workstation to establish the Antivirus Product name, Scanning status, Up-to-date status, and Version number.
Scan Interval (Minutes)	5 minutes (default), 60 minutes (maximum)

Status Details

AV - Security Center

Status Detail	Description
Antivirus Product Name	Identifies the antivirus software being monitored (normally including both the vendor name as well as the specific product name).
Virus Scanning Enabled	Indicates whether the antivirus software is currently actively scanning or if it has been disabled.
Antivirus Product Up-to-Date	Indicates whether the virus dictionary being used by the antivirus software is current or outdated.
Version Number	The release identifier of the antivirus software being monitored.

Chapter 5

Antivirus Activity

The Antivirus Activity (AV Activity) services monitor the scanning activities of the following anti-virus applications:

- McAfee® VirusScan® Enterprise 7.1
- McAfee® VirusScan® Enterprise 8.0i
- Sophos Anti-Virus NT/2000/XP/2003 3.xx
- Sophos Anti-Virus for Windows 2000/XP/2003 5.0
- Symantec® Antivirus® Corporate Edition 9.0 and 10.0
- Trend Micro™ ServerProtect™ 5.58

During the monitoring process, an anti-virus application scans the device on which it is installed and records any security-specific events in a local log file. The N-central agent that is used for an anti-virus activity service scans the log file for any keywords that match the regular expressions specified for the service. The agent scans only the events that have been logged since the last execution of the service scan. If a match is found, the agent reports it to the central server, and based on the specified thresholds, N-central displays the appropriate status for the service.

If the status triggers a notification, the notification includes the first line and the line numbers on which the keyword was found. The first line and any subsequent line numbers are also displayed in the applicable reports and on the status details screen for the service. These services support wide characters.

AV Activity - McAfee

Service Type:	Security
Collection Method:	Log Appended
Instances on a Device:	Single
Supported Platforms:	McAfee® VirusScan® Enterprise 7.1
Device Class:	Generic Server, Generic Workstation, Windows Server, and Windows Workstation
Monitored By:	Central Server (Agent: Windows)
Service Version:	N-central 4.0 and greater

For information about the monitoring process, refer to Antivirus Activity on page 15.

Service Details

AV Activity - McAfee Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Log File Name and Path	
Start Time	
End Time	
Scan Interval (Minutes)	
Repeat Weekly on Day(s)	
Repeat Monthly on Day(s)	
Regular Expression 1 for "Virus found”	Alerts you when the anti-virus application has detected a virus.
Regular Expression 2 for "Files moved"	Alerts you when the anti-virus application has moved affected files to a “quarantined” location.
Regular Expression 3 for "Files cleaned or deleted"	Alerts you when the anti-virus application has cleaned or deleted the affected files.
Regular Expressions 4, 5, and 6	Refer to Table 1-1 on page 2.

Status Details

AV Activity - McAfee Status Details

Status Detail	Description
Virus found	The threshold values that determine the status change of the service. If the related regular expression is found, the test is successful. Otherwise, the test is unsuccessful. Based on the test results, the appropriate status is then displayed for the service.
Files moved	
Files cleaned or files deleted	
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	The first 250 characters of the first line, in the log file, containing the matching keyword returned by the agent. This information is displayed on the service’s status details screen, any applicable reports, and any triggered notifications (except for numeric pages).

AV Activity - McAfee 8

Service Type: Security

Collection Method: Log Appended

Instances on a Device: Single

Supported Platforms:	McAfee® VirusScan® Enterprise 8.0i
Device Class:	Generic Server, Generic Workstation, Windows Server, and Windows Workstation
Monitored By:	Central Server (Agent: Windows)
Service Version:	N-central 4.0 and greater

For information about the monitoring process, refer to Antivirus Activity on page 15.

Service Details

AV Activity - McAfee 8 Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Log File Name and Path	
Start Time	
End Time	
Scan Interval (Minutes)	
Repeat Weekly on Day(s)	
Repeat Monthly on Day(s)	
Regular Expression 1 for "Virus found”	Alerts you when the anti-virus application has detected a virus.
Regular Expression 2 for "Files moved"	Alerts you when the anti-virus application has moved affected files to a “quarantined” location.
Regular Expression 3 for "Files cleaned or deleted"	Alerts you when the anti-virus application has cleaned or deleted the affected files.
Regular Expressions 4, 5, and 6	Refer to Table 1-1 on page 2.

Status Details

AV Activity - McAfee 8 Status Details

Status Details	Description
Virus found	The threshold values that determine the status change of the service. If the related regular expression is found, the test is successful. Otherwise, the test is unsuccessful. Based on the test results, the appropriate status is then displayed for the service.
Files moved	
Files cleaned or files deleted	

Status Details	Description
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	The first 250 characters of the first line, in the log file, containing the matching keyword returned by the agent. This information is displayed on the service's status details screen, any applicable reports, and any triggered notifications (except for numeric pages).

AV Activity - Sophos

Service Type: Security

Collection Method: Log Appended

Instances on a Device: Single

Supported Platforms: Sophos Anti-Virus for Windows NT/2000/XP/2003 3.xx

Device Class: Generic Server, Generic Workstation, Windows Server, and Windows Workstation

Monitored By: Agent (Windows))

Service Version: N-central 4.0 and greater

For information about the monitoring process, refer to Antivirus Activity on page 15.

Service Details

AV Activity - Sophos Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Log File Name and Path	
Start Time	
End Time	
Scan Interval (Minutes)	
Repeat Weekly on Day(s)	
Repeat Monthly on Day(s)	
Regular Expression 1 for "No virus found"	Alerts you when the anti-virus application has not detected a virus.
Regular Expression 2 for "Virus found"	Alerts you when the anti-virus application has detected a virus.
Regular Expression 3 for "Virus found and fix unsuccessful"	Alerts you when the anti-virus application has located an infected file, but failed to fix it.

Service Detail	Description
Regular Expression 4 for "Virus found and fix successful"	Alerts you when the anti-virus application has located and fixed an infected file.
Regular Expressions 5 and 6	Refer to Table 1-1 on page 2.

Status Details

AV Activity - Sophos Status Details

Status Detail	Description
No virus found	The threshold values that determine the status change of the service. If the related regular expression is found, the test is successful. Otherwise, the test is unsuccessful. Based on the test results, the appropriate status is then displayed for the service.
Virus found	
Virus found and fix unsuccessful	
Virus found and fix successful	
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	The first 250 characters of the first line, in the log file, containing the matching keyword returned by the agent. This information is displayed on the service's status details screen, any applicable reports, and any triggered notifications (except for numeric pages).

AV Activity - Sophos 5

Service Type: Security

Collection Method: Log Appended

Instances on a Device: Single

Supported Platforms: Sophos Anti-Virus for Windows 2000/XP/2003 5.0

Device Class: Generic Server, Generic Workstation, Windows Server, and Windows Workstation

Monitored By: Agent (Windows))

Service Version: N-central 4.0 and greater

For information about the monitoring process, refer to Antivirus Activity on page 15.

Service Details

AV Activity - Sophos 5 Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Log File Name and Path	
Start Time	
End Time	
Scan Interval (Minutes)	
Repeat Weekly on Day(s)	
Repeat Monthly on Day(s)	
Regular Expression 1 for "No virus found”	Alerts you when the anti-virus application has not detected a virus.
Regular Expression 2 for "Virus found"	Alerts you when the anti-virus application has detected a virus.
Regular Expression 3 for "Virus found and fix unsuccessful"	Alerts you when the anti-virus application has located an infected file, but failed to fix it.
Regular Expression 4 for "Virus found and fix successful"	Alerts you when the anti-virus application has located and fixed an infected file.
Regular Expressions 5 and 6	Refer to Table 1-1 on page 2.

Status Details

AV Activity - Sophos 5 Status Details

Status Detail	Description
No virus found	The threshold values that determine the status change of the service. If the related regular expression is found, the test is successful. Otherwise, the test is unsuccessful. Based on the test results, the appropriate status is then displayed for the service.
Virus found	
Virus found and fix unsuccessful	
Virus found and fix successful	
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	The first 250 characters of the first line, in the log file, containing the matching keyword returned by the agent. This information is displayed on the service’s status details screen, any applicable reports, and any triggered notifications (except for numeric pages).

AV Activity - Symantec

Service Type: Security

Collection Method: Log Appended

Instances on a Device: Single

Supported Platforms: Symantec Antivirus Corporate Edition 9.0 and 10.0, and Norton® AntiVirus® Corporate Edition 7.6 (if the name of its log file has been specified.)

Device Class: Generic Server, Generic Workstation, Windows Server, and Windows Workstation

Monitored By: Agent (Windows))

Service Version: N-central 4.0 and greater

For information about the monitoring process, refer to Antivirus Activity on page 15.

Service Details

AV Activity - Symantec Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Log File Name and Path	
Start Time	
End Time	
Scan Interval	
Repeat Weekly on Day(s)	
Repeat Monthly on Day(s)	
Regular Expression 1 for “Quarantined file”	Alerts you when the anti-virus application has quarantined an infected file.
Regular Expression 2 for “Renamed file”	Alerts you when the anti-virus application has renamed an infected file as part of its process for removing the virus.
Regular Expression 3 for “Deleted infected file”	Alerts you when the anti-virus application has removed an infected file.
Regular Expression 4 for “Logged corrupt file”	Alerts you when the anti-virus application has only logged an infected file. Further action may not be taken if the anti-virus application does not have a solution for the logged file or if it has been configured not to clean an infected file.
Regular Expression 5 for “Cleaned and removed file (virus)”	Alerts you when a virus has been successfully removed from a file.
Regular Expression 6 for “Cleaned and removed file (macro virus)”	Alerts you when an identified macro virus has been removed from a file.

Status Details

AV Activity - Symantec Status Details

Status Detail	Description
Quarantined file	The threshold values that determine the status change of the service. If the related regular expression is found, the test is successful, otherwise it is unsuccessful. Based on the test results, the appropriate status is then displayed for the service.
Renamed file	
Deleted infected file	
Logged corrupt file	
Cleaned and removed file (virus)	
Cleaned and removed file (macro virus)	
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	The first 250 characters of the first line, in the log file, containing the matching keyword returned by the agent. This information is displayed on the service's status details screen, any applicable reports, and any triggered notifications (except for numeric pages).

AV Activity - Trend Micro

Service Type: Security

Collection Method: Log Appended

Instances on a Device: Single

Supported Platforms: STrend Micro™ ServerProtect™ 5.58

Device Class: Generic Server, Generic Workstation, Windows Server, and Windows Workstation

Monitored By: Agent (Windows))

Service Version: N-central 4.0 and greater

For information about the monitoring process, refer to Antivirus Activity on page 15.

Service Details

AV Activity - Trend Micro Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Log File Name and Path	The name and location of the log file that was specified when setting options to export the scanned data to a log file.

Service Detail	Description
Start Time	The start time of the scan. The start time should be scheduled one hour after the time scheduled for the data export to the specified log file. For example, if the data export was scheduled for 4:00 p.m., the scan start time should be scheduled for 5:00 p.m.
End Time	The end time of the scan. The End Time should be set to 00.
Scan Interval	The time (in minutes) between each scan. The Scan Interval should be set to 00.
Repeat Weekly on Day(s)	Refer to Table 1-1 on page 2.
Repeat Monthly on Day(s)	
Regular Expression 1 for “Quarantine success”	Alerts you when the anti-virus application has quarantined an infected file.
Regular Expression 2 for “Clean success”	Alerts you when a virus has been successfully removed from a file.
Regular Expression 3 for “Delete success”	Alerts you when the anti-virus application has removed an infected file.
Regular Expression 4 for “Pass success”	Alerts you when the anti-virus application has not scanned a file due to a unique message ID.
Regular Expression 5 for “Rename success”	Alerts you when the anti-virus application has renamed an infected file as part of its process for removing the virus.
Regular Expression 6	Refer to Table 1-1 on page 2.

Status Details

AV Activity - Trend Micro Status Details

Status Detail	Description
Quarantine success	The threshold values that determine the status change of the service. If the related regular expression is found, the test is successful. Otherwise, the test is unsuccessful. Based on the test results, the appropriate status is then displayed for the service.
Clean success	
Delete success	
Pass success	
Rename success	
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	The first 250 characters of the first line, in the log file, containing the matching keyword returned by the agent. This information is displayed on the service’s status details screen, any applicable reports, and any triggered notifications (except for numeric pages).

Setting Up the Trend Micro Services

Before the AV Activity or Definition Trend Micro services can monitor the TrendMicro ServerProtect application, you must install TrendMicro Information Server and ServerProtect 5.58 and set up ServerProtect by performing the following five tasks:

a. To schedule the downloads of the Update files

b. To schedule the deployment of the Update files

c. To schedule a virus scan

d. To export the scanned data to a log file

e. To set up the service, refer to Editing Services in the *Customer Manual*.

To schedule the downloads of the Update files

1. Click Start>Programs>TrendMicro ServerProtect Management Console>ServerProtect Management Console.
   ↳ The Trend Micro ServerProtect Management Console dialog appears.
2. Type the password of the Information Server.
3. Click OK.
   ↳ The Trend Micro ServerProtect Management Console appears.
4. On the Task side bar, click Update.
   ↳ The Update and Rollback icons appear.
5. Click the Update icon.
   ↳ The Update screen appears.
6. In the Download section, click Configure.
   ↳ The Download Option dialog appears.
7. Click the Schedule Setting tab.
8. For the Frequency field, select Daily.
9. Specify the Time at which you would like to download the Update files.
10. Click OK.
    ↳ The download schedule of the Update files is set and the Update screen appears.
11. Proceed to To schedule the deployment of the Update files on page 24.

To schedule the deployment of the Update files

1. In the Deploy section, click Configure.
   ↳ The Deploy Option dialog appears.
2. Click New task.
   ↳ The New Task screen appears.
3. In the right panel of the New Task screen, click Create.
   ↳ The Create New Tasks dialog appears.

4. In the Existing tasks column, select Deploy.
5. Click Add #1 task item.
   ↳ The Deploy option appears in the Selected task(s) column.
6. Select Create as a scheduled task.
7. Click Create.
   ↳ The Task Wizard appears.
8. Click Next.
9. For the Frequency field, select Daily.
10. Specify the Time at which you would like to deploy the Update files.

    Note: We recommend that you schedule the deployment of the Update files one hour after the download of the Update files. For example, if you scheduled the download of the Update files for 1:00 p.m., you should schedule the deployment for 2:00 p.m.
11. Click Next.
    ↳ The Update Settings dialog appears.
12. Select all three deployment tasks: Virus pattern, Scan engine, and Program.
13. Click Next.
    ↳ The Task Information dialog appears.
14. Specify the Task name.
15. Specify the Task owner.
16. Click Finish.
    ↳ The New Task screen appears.

    Tip: *You can click the* Existing Task *icon on the Task side bar to view the new task you created in the left panel of the* Existing Task *screen.*
17. Proceed to To schedule a virus scan on page 25.

To schedule a virus scan

1. In the right panel of the New Task screen, click Create.
   ↳ The Create New Tasks dialog appears.
2. In the Existing tasks column, select Scan Now.
3. Click Add #1 task item.
   ↳ The Scan Now option appears in the Selected task(s) column.
4. Select Create as a scheduled task.
5. Click Create.
   ↳ The Task Wizard appears.
6. Click Next.
7. For the Frequency field, select Daily.

8. Specify the Time at which you would like to schedule the virus scan.

   Note: We recommend that you schedule the virus scan one hour after the deployment of the Update files. For example, if you scheduled the deployment of the Update files for 2:00 p.m., you should schedule the virus scan for 3:00 p.m.

9. Click Next.

   ↳ The On-demand Scanning Target appears.

10. Select All drives to be scanned.
11. Click Next.

    ↳ The Select Profile dialog appears.

12. Configure as required and click Next.
13. Repeat step 12 until the Task Information dialog appears.
14. Specify the Task name.
15. Specify the Task owner.
16. Click Finish.

    ↳ The New Task screen appears.

    Tip: *You can click the* Existing Task *icon on the Task side bar to view the task you created in the left panel of the* Existing Task *screen.*

17. Proceed to To export the scanned data to a log file on page 26.

To export the scanned data to a log file

1. In the right panel of the New Task screen, click Create.

   ↳ The Create New Tasks dialog appears.

2. In the Existing tasks column, select Export logs.
3. Click Add #1 task item.

   ↳ The Export logs option appears in the Selected task(s) column.

4. Select Create as a scheduled task.
5. Click Create.

   ↳ The Task Wizard appears.

6. Click Next.
7. Select Daily as the Frequency.
8. Specify the Time at which you would like to export the scanned data to the log file.

   Note: We recommend that you schedule the export one hour after the virus scan. For example, if you scheduled the virus scan for 3:00 p.m., you should schedule the export for 4:00 p.m.

9. Click Next.

   ↳ The Exported Log Settings dialog appears.

10. Select all of the Log types that you would like to export to the log file: Infections, Scan summary, System, Update, Alert, and Task.

11. Click Next.
12. Specify the Exported CSV file name. For example: Admin
13. Click Next.
    ↳ The Task Information dialog appears.
14. Specify the Task name.
15. Specify the Task owner.
16. Click Finish.
    ↳ The scanned data is exported to the specified file and the New Task screen appears.

    Tip: *You can click the* Existing Task *icon on the Task side bar to view the task you created in the left panel of the* Existing Task *screen.*
17. To set up the service, refer to Editing Services in the *Customer Manual*.

Chapter 6

Antivirus Definition

The Antivirus Definition (AV Def.) services monitor the update events of the following anti-virus applications:

- McAfee® VirusScan® Enterprise 7.1
- McAfee® VirusScan® Enterprise 8.0i
- Sophos Anti-Virus NT/2000/XP/2003 3.xx
- Sophos Anti-Virus 2000/XP/2003 5.0
- Symantec® Antivirus® Corporate Edition 9.0 and 10.0
- Trend Micro™ ServerProtect™ 5.58

The anti-virus application sends update events as they occur to a local log file. From N-central, the agent that is used for an anti-virus definition service scans the respective log file for any keywords that match the regular expressions specified for the service. The agent scans only the events that have been logged since the last execution of the service scan. If a match is found, the agent reports it to the central server, and based on the specified thresholds, N-central displays the appropriate status for the service.

If the status triggers a notification, the notification includes the first line and the line numbers on which the keyword was found unless a numeric pager was used for the notification. The first line and any subsequent line numbers are also displayed in the applicable reports and on the status details screen for the service. These services support wide characters.

AV Def. - McAfee

Service Type:	Security
Collection Method:	Log Appended
Instances on a Device:	Single
Supported Platforms:	McAfee® VirusScan® Enterprise 7.1
Device Class:	Generic Server, Generic Workstation, Windows Server, and Windows Workstation
Monitored By:	Agent (Windows)
Service Version:	N-central 4.0 and greater

For information about the monitoring process, refer to Antivirus Definition on page 29.

Service Details

AV Def. - McAfee Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Log File Name and Path	The name and location of the log file that was specified when setting options to export the scanned data to a log file.
Start Time	The start time of the scan. The start time should be scheduled one hour after the time scheduled for the data export to the specified log file. For example, if the data export was scheduled for 4:00 p.m., the scan start time should be scheduled for 5:00 p.m.
End Time	
Scan Interval	
Repeat Weekly on Day(s)	
Repeat Monthly on Day(s)	
Regular Expression 1 for “Update success”	Alerts you when the definition file of the anti-virus application has been automatically updated.
Regular Expression 2 for “Update success”	
Regular Expression 3 for “Update success”	
Regular Expression 4 for “Update success”	
Regular Expression 5 for “Update success”	
Regular Expression 6 for “Update failed”	Alerts you when the update of the definition file was unsuccessful.

Status Details

AV Def. - MacAfee Status Details

Status Detail	Description
Regular expressions 1 to 5 “Update success”	The threshold values that determine the status change of the service. If the related regular expression is found, the test is successful. Otherwise, the test is unsuccessful. Based on the test results, the appropriate status is then displayed for the service.
Regular expression 6 “Update failed”	

Status Detail	Description
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications(except for numeric pages).
The first line matched	The first 250 characters of the first line, in the log file, containing the matching keyword returned by the agent. This information is displayed on the service's status details screen, any applicable reports, and any triggered notifications (except for numeric pages).

AV Def. - McAfee 8

Service Type: Security

Collection Method: Log Appended

Instances on a Device: Single

Supported Platforms: McAfee® VirusScan® Enterprise 8.0i

Device Class: Generic Server, Generic Workstation, Windows Server, and Windows Workstation

Monitored By: Agent (Windows)

Service Version: N-central 4.0 and greater

For information about the monitoring process, refer to Antivirus Definition on page 29.

Service Details

AV Def. - McAfee 8 Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Log File Name and Path	The name and location of the log file that was specified when setting options to export the scanned data to a log file.
Start Time	The start time of the scan. The start time should be scheduled one hour after the time scheduled for the data export to the specified log file. For example, if the data export was scheduled for 4:00 p.m., the scan start time should be scheduled for 5:00 p.m.
End Time	
Scan Interval	
Repeat Weekly on Day(s)	
Repeat Monthly on Day(s)	

Service Detail	Description
Regular Expression 1 for “Update success”	Alerts you when the definition file of the anti-virus application has been automatically updated.
Regular Expression 2 for “Update success”	
Regular Expression 3 for “Update success”	
Regular Expression 4 for “Update success”	
Regular Expression 5 for “Update success”	
Regular Expression 6 for “Update failed”	Alerts you when the update of the definition file was unsuccessful.

Status Details

AV Def. - McAfee 8 Status Details

Status Details	Description
Regular expressions 1 to 5 “Update success”	The threshold values that determine the status change of the service. If the related regular expression is found, the test is successful. Otherwise, the test is unsuccessful. Based on the test results, the appropriate status is then displayed for the service.
Regular expression 6 “Update failed”	
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	The first 250 characters of the first line, in the log file, containing the matching keyword returned by the agent. This information is displayed on the service’s status details screen, any applicable reports, and any triggered notifications (except for numeric pages).

AV Def. - Sophos

Service Type: Security

Collection Method: Log Appended

Instances on a Device: Single

Supported Platforms: Sophos Anti-Virus for Windows NT/2000/XP/2003 3.xx

Device Class: Generic Server, Generic Workstation, Windows Server, and Windows Workstation

Monitored By: Agent (Windows)

Service Version: N-central 4.0 and greater

For information about the monitoring process, refer to Antivirus Definition on page 29.

Service Details

AV Def. - Sophos Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Log File Name and Path	
Start Time	
End Time	
Scan Interval	
Repeat Weekly on Day(s)	
Repeat Monthly on Day(s)	
Regular Expression 1 for “Update started”	Alerts you when the update of the definition file has started.
Regular Expressions 2 to 6	Refer to Table 1-1 on page 2.

Status Details

AV Def. - Sophos Status Details

Status Detail	Description
Update Started	The threshold value that determines the status change of the service. If the related regular expression is found, the test is successful. Otherwise, the test is unsuccessful. Based on the test results, the appropriate status is then displayed for the service.
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	The first 250 characters of the first line, in the log file, containing the matching keyword returned by the agent. This information is displayed on the service’s status details screen, any applicable reports, and any triggered notifications (except for numeric pages).

AV Def. - Sophos 5

Service Type: Security

Collection Method: Log Appended

Instances on a Device: Single

Supported Platforms: Sophos Anti-Virus for Windows 2000/XP/2003 5.0

Device Class: Generic Server, Generic Workstation, Windows Server, and Windows Workstation

Monitored By: Agent (Windows)

Service Version: N-central 4.0 and greater

For information about the monitoring process, refer to Antivirus Definition on page 29.

Service Details

AV Def. - Sophos 5 Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Log File Name and Path	
Start Time	
End Time	
Scan Interval	
Repeat Weekly on Day(s)	
Repeat Monthly on Day(s)	
Regular Expression 1 for “Update started”	Alerts you when the update of the definition file has started.
Regular Expression 2 for “Update completed”	Alerts you when the update of the definition file has completed.
Regular Expression 3 for “Update failed”	Alerts you when the update of the definition file has failed.
Regular Expressions 4 to 6	Refer to Table 1-1 on page 2.

Status Details

AV Def. - Sophos 5 Status Details

Status Detail	Description
Update Started	The threshold value that determines the status change of the service. If the related regular expression is found, the test is successful. Otherwise, the test is unsuccessful. Based on the test results, the appropriate status is then displayed for the service.
Update Complete	The threshold value that determines the status change of the service. If the related regular expression is found, the test is successful. Otherwise, the test is unsuccessful. Based on the test results, the appropriate status is then displayed for the service.
Update Failed	The threshold value that determines the status change of the service. If the related regular expression is found, the test is successful. Otherwise, the test is unsuccessful. Based on the test results, the appropriate status is then displayed for the service.

Status Detail	Description
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	The first 250 characters of the first line, in the log file, containing the matching keyword returned by the agent. This information is displayed on the service's status details screen, any applicable reports, and any triggered notifications (except for numeric pages).

AV Def. - Symantec

Service Type: Security

Collection Method: Log Appended

Instances on a Device: Single

Supported Platforms: Symantec Antivirus Corporate Edition 8.0 and Norton® AntiVirus® Corporate Edition 7.6 (if the name of its log file has been specified.)

Device Class: Generic Server, Generic Workstation, Windows Server, and Windows Workstation

Monitored By: Agent (Windows)

Service Version: N-central 4.0 and greater

For information about the monitoring process, refer to Antivirus Definition on page 29.

Service Details

AV Def. - Symantec Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Scan Interval	
Log File Name and Path	
Regular Expression 1 for "Patches found and applied"	Alerts you if the anti-virus application identified and applied patches to the installed applications. If this entry does not appear, it does not indicate a failure; it can indicate that there were no patches applied. The Virus Definition may be up-to-date.
Regular Expression 2 for "Issue contacting the Update Server"	Alerts you when proper connection to the LiveUpdate server could not be established.
Regular Expression 3 for "Issue extracting the update zip file"	Alerts you when the task of extracting the update zip file could not be completed.

Status Detail

AV Def. - Symantec Status Details

Status Detail	Description
Patches were found and applied	The threshold values that determine the status change of the service. If the related regular expression is found, the test is successful. Otherwise, the test is unsuccessful. Based on the test results, the appropriate status is then displayed for the service.
Issue contacting LiveUpdate server	
Issue extracting update zip file	
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	The first 250 characters of the first line, in the log file, containing the matching keyword returned by the agent. This information is displayed on the service's status details screen, any applicable reports, and any triggered notifications (except for numeric pages).

AV Def. - Trend Micro

Service Type: Security

Collection Method: Log Batch

Instances on a Device: Single

Supported Platforms: Trend Micro™ ServerProtect™ 5.58

Device Class: Generic Server, Generic Workstation, Windows Server, and Windows Workstation

Monitored By: Agent (Windows)

Service Version: N-central 4.0 and greater

For information about the monitoring process, refer to Antivirus Definition on page 29.

Service Details

AV Def. - Trend Micro Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Log File Name and Path	The name and location of the log file that was specified when setting options to export the scanned data to a log file.

Service Detail	Description
Start Time	The start time of the scan. The start time should be scheduled one hour after the time scheduled for the data export to the specified log file. For example, if the data export was scheduled for 4:00 p.m., the scan start time should be scheduled for 5:00 p.m.
End Time	The end time of the scan. The End Time should be set to 00.
Scan Interval	The time (in minutes) between each scan. The Scan Interval should be set to 00.
Repeat Weekly on Day(s)	Refer to Table 1-1 on page 2.
Repeat Monthly on Day(s)	
Regular Expression 1 for “Update success”	Alerts you when the definition file of the anti-virus application has been automatically updated.
Regular Expressions 2 to 6	Refer to Table 1-1 on page 2.

Status Details

AV Def. - Trend Micro Status Details

Status Detail	Description
Update success	The threshold value that determines the status change of the service. If the related regular expression is found, the test is successful. Otherwise, the test is unsuccessful. Based on the test results, the appropriate status is then displayed for the service.
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	The first 250 characters of the first line, in the log file, containing the matching keyword returned by the agent. This information is displayed on the service’s status details screen, any applicable reports, and any triggered notifications (except for numeric pages).

Setting Up the Trend Micro Services

The TrendMicro ServerProtect application can be monitored by the AV Activity and Definition Trend Micro services only after it is set up with specific options. For information about setting up this service, refer to Setting Up the Trend Micro Services on page 24.

Chapter 7
APC UPS

Service Type: Network

Collection Method: SNMP

Instances on a Device: Single

Supported Platforms: Any PowerNet-MIB Compliant Device from APC

Device Class: Generic Server, Other, Printer, Scanner/Camera, Switch/Router, and Windows Server

Monitored By: Hardware Probe, Windows Probes

Service Version: N-central 5.0 and greater

The ACP UPS service provides basic and advanced APC UPS battery information.

Service Details

APC UPS Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	

Status Details

APC UPS Status Details

Status Detail	Description
Status	The status of the UPS batteries. A batteryLow(3) value indicates the UPS will be unable to sustain the current load, and its services will be lost if power is not restored: • unknown(1) translates to Warning, • batteryNormal(2) translates to Normal, • batteryLow(3) translates to Failed.
Time On	The elapsed time since the UPS has switched to battery power, expressed in hundredths of a second.
Last Replaced	The date when the UPS system's batteries were last replaced, in mm/dd/yy format. For Smart-UPS models, this value is originally set in the factory. When the UPS batteries are replaced, this value should be reset by the administrator.
Capacity	The remaining battery capacity expressed in percent of full capacity.
Temperature	The current internal UPS temperature, expressed in Celsius.
Time Remaining	The UPS battery run time remaining before battery exhaustion, expressed in hundredths of a second.
Replace Indicator	Indicates if the UPS batteries need to be replaced: • noBatteryNeedsReplacing(1) translates to Normal, • batteryNeedsReplacing(2) translates to Failed.

Chapter 8

Application Compliance

Service Type: Security

Collection Method: WMI Workstation

Instances on a Device: Single

Supported Platforms: Windows®

Device Class: Windows Server and Windows Workstation

Monitored By: Network Windows Probe, Workgroup Windows Probe, WSP

Service Version: N-central 3.6 and greater

Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* published by Microsoft®.

The Application Compliance service ensures that your organization's network complies with your organization's software policies. By ensuring continued policy compliance, this service helps you protect your organization from outside threats and the use of unauthorized software.

During the monitoring process, the Application Compliance service collects the names of the installed applications from the Windows registry and compares them with a default list of applications that is approved by your organization. This list of names are entered by your administrator. When the service detects an application name that is not on the list of approved application names, it changes to a configured state.

Service Details

Application Compliance Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	

Service Detail	Description
Scan Interval	The time (in minutes) between each scan. This value must be equal to or greater than 360 minutes and equal to or less than 1440 minutes.
Application List	The names of the applications that you would like to monitor, using the comma separated value (CSV) format. This field allows a maximum of 8 KB. If you specify a name that has a comma, when setting up the service, N-central replaces the comma with a space.
Application List (Cont)	If the content in the Application List field has reached its maximum, you can continue adding the names of the applications, that you would like to monitor in these fields in CSV format. Each name must be contained within one field. It must not be split across fields. Each field allows a maximum of 8 KB.
Application List (Cont)	
Application List (Cont)	
Application List (Cont)	

Status Details

Application Compliance Status Details

Status Detail	Description
Applications are in Compliance	Displays the list of applications that are non-compliant. Notifies when an unauthorized application has been identified.

Chapter 9

Backup Exec

Service Type: System

Collection Method: ODBC

Instances on a Device: Multiple

Supported Platforms: Veritas™ Backup Exec™, up to version 10

Device Class: Generic Server and Windows Server

Monitored By: Agent (Windows), Workgroup Windows Probe, WSP

Service Version: N-central 5.0 and greater

The Backup Exec service monitors the results of the discovered jobs that have been performed by Veritas™ Backup Exec™ and recorded in the Veritas MS SQL database. Using the Open Database Connectivity (ODBC), which is a standard application program interface (API), the Backup Exec service can monitor up to 10 jobs.

The Backup Exec service can monitor the following types of jobs: backup, catalog, report, restore, set copy, test run, utility, and verify.

For the Backup Exec service to work properly, ensure that:

- The user credentials used by the Windows Probe to login to the Veritas database must have "db_datareader" rights. For more information, refer to Enabling Rights to the Veritas Database on page 45;
- the Microsoft Data Access Components (MDAC) version 2.8 or greater is installed for the job discovery;
- the MDAC contains the ODBC driver manager and MS SQL ODBC driver, which are required to connect to the Veritas MS SQL database; and
- the Microsoft SQL server is set up in “mixed mode”. For more information, refer to Setting Up the SQL Server in Mixed Mode on page 45.

The table Job StatusTypes lists the jobs that are discovered and monitored by the Backup Exec service.

Job StatusTypes

Job Status Type	Database Table	Parameter
backup	BackupJobInstance	1
catalog	CatalogJobInstance	2
report	ReportJobInstance	3
restore	RestoreJobInstance	4

Job Status Type	Database Table	Parameter
set copy	SetCopyJobInstance	5
test run	TestRunJobInstance	6
utility	UtilityJobInstance	7
verify	VerifyJobInstance	8

Service Details

Backup Exec Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Job GUID to Monitor	The unique ID of the job to monitor. (read-only) Example: {4BC69ECD-06A2-492D-BC37-5A6CC6E7B638}
Failed Job Status List	The list of Failed job statuses.
Warning Job Status List	The list of Warning job statuses.
Job Name to Monitor	The name of the job to monitor (read-only).
Job Type	The type of Veritas job being performed.
Start Time	Refer to Table 1-1 on page 2.
End Time	
Scan Interval in Minutes	
Repeat Day	
Repeat Month Days	

Status Details

Backup Exec Status Details

Status Detail	Description
Backup Exec Job Return Code	The return value that is based on the job status of the backup.
Elapsed Time	The time taken to perform the backup.
Number of directories backed up	The details of a backup.
Number of files backed up	
Number of files skipped	
Number of files corrupted	
Number of files in use	The details of a backup.
Total bytes backed up	
Byte rate (MB per minute)	The speed of a backup.

Backup Exec 10 Job Status

You can view the return values for the associated job status on the status screen for the Backup Exec service. These values represent specific critical issues. For more information about these values, refer to Job Status for Veritas 9 and 10 on page 253.

Setting Up the SQL Server in Mixed Mode

Before the Backup Exec service can monitor the results of the discovered jobs that have been performed by the MS SQL database, you must set up the SQL server in “mixed mode”.

Warning! The following changes should be reviewed, approved, and implemented by a Microsoft certified professional. For more information about switching the SQL Server to Mixed Mode, contact Microsoft Corporation.

To set up the SQL server in mixed mode

1. Click Start>All Programs>Microsoft SQL Server>Enterprise Manager.
   ↳ The SQL Server Enterprise Manager screen appears.
2. Navigate to the appropriate SQL Server Group.
3. In the contents pane, right-click the appropriate SQL server.
4. Click Properties.
   ↳ The SQL Server Properties dialog appears.
5. Select the Security tab.
   ↳ The Security tab contents display.
6. Under the Security heading, locate the Authentication section and select SQL Server and Windows.
7. Click OK.

Enabling Rights to the Veritas Database

The Windows probe user must have rights to the Veritas database enabled before they can log in to the Veritas database.

Warning! The following changes should be reviewed, approved, and implemented by a Microsoft certified professional. For more information, contact Microsoft Corporation.

To enable rights to the Veritas database

1. Click Start>All Programs>Microsoft SQL Server>Enterprise Manager
   ↳ The SQL Server Enterprise Manager screen appears.
2. In the navigation pane, drill to Databases.
3. Select the appropriate Veritas database.
4. Click Users.
5. In the contents pane, right-click the appropriate user.

6. Click Properties.
   ↳ The Database User Properties screen appears.
7. Click the General tab.
   ↳ The contents of the General tab display.
8. On the General tab, select db_datareader.
9. Click OK.
   ↳ The Veritas user rights are configured.

Chapter 10

CCM Analog Gateway

Service Type: VoIP

Collection Method: WMI

Instances on a Device: Single

Supported Platforms: Cisco® CallManager Version 4.1

Device Class: Windows Server

Monitoring Probe: Network Windows Probe, Workgroup Windows Probe, and WSP

Monitoring Probe Version: 4.5 SP1 and greater

The Cisco CallManager (CCM) Analog Gateway service monitors the state of the different ports on the gateway that is connected to the Call Manager.

Service Details

CCM Analog Gateway Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Service Description	
Scan Interval	

Status Details

CCM Analog Gateway Status Details

Status Detail	Description
FXO Ports in Service	The total number of Foreign eXchange Office (FXO) ports that are currently available for use.
FXO Ports Active	The total number of FXO ports that are currently registered with the CallManager and are in use (active).
FXO Port Utilization (%)	A calculated percentage of the FXO port utilization: FXO Ports Active * 100/(FXO Ports Active + FXO Ports in Service)
FXS Ports in Service	The total number of Foreign eXchange Subscriber (FXS) ports that are currently available for use.

Status Detail	Description
FXS Ports Active	The total number of FXS ports that are currently registered with the CallManager and are in use (active).
FXS Port Utilization (%)	A calculated percentage of the FXS port utilization: FXS Ports Active * 100/(FXS Ports Active + FXS Ports in Service)

Chapter 11
CCM Annunciator

Service Type:	VoIP
Collection Method:	WMI
Instances on a Device:	Single
Supported Platforms:	Cisco® CallManager Version 4.1
Device Class:	Windows Server
Monitoring Probe:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, and WSP
Monitoring Probe Version:	4.5 SP1 and greater

The Cisco CallManager (CCM) Annunciator service monitors the state of the resources associated with the call recorded announcements that are connected to the CallManager.

If the Total Annunciator Resources is greater than 0, the service status is Normal.

If the Annunciator Out of Resources Incidents is 30% or less than the Total Annunciator Resources, the service status is Warning.

If the Annunciator Out of Resources Incidents is a value other than 0 and the Available Annunciator Resources percentage is 10% or less than the Total Annunciator Resources, the service status is Failed.

Service Details

CCM Annunciator Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Service Description	
Scan Interval	

Status Details

CCM Annunciator Status Details

Status Detail	Description
Total Annunciator Resources	The total number of resources for all of the devices.
Available Annunciator Resources	The total number of annunciator resources that are currently registered with the CallManager and are in use (active).
Active Annunciator Resources	The total number of annunciator resources that are currently registered with the CallManager and are not in use (available).
Annunciator Resources Utilization (%)	A calculated percentage of the annunciator resources utilization: Active Annunciator Resources * 100 / Total Annunciator Resources
Annunciator Out of Resources Incidents	The total number of attempts made to find an annunciator resource when all other registered annunciator resources were in use.

Chapter 12

CCM Call Activity

Service Type: VoIP

Collection Method: WMI

Instances on a Device: Single

Supported Platforms: Cisco® CallManager Version 4.1

Device Class: Windows Server

Monitoring Probe: Network Windows Probe, Workgroup Windows Probe, and WSP

Monitoring Probe Version: 4.5 SP1 and greater

The Cisco CallManager (CCM) Call Activity service monitors the state of all calls on the Call Manager. This includes the active calls, attempted calls, calls in progress, and completed calls.

Service Details

CCM Call Activity Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Service Description	
Scan Interval	

Status Details

CCM Call Activity Status Details

Status Detail	Description
Active Calls	The number of active calls.
Attempted Calls	The number of attempted calls.
Completed Calls	The number of completed calls.
Calls in Progress	The number of calls in progress.
Authenticated Active Calls	The total number of calls that have been authenticated and are in progress.

Status Detail	Description
Authenticated Calls Completed	The total number of authenticated calls that have been terminated.
Calls Active + Calls Completed	Total number of calls in progress + Total number of calls terminated.

Chapter 13

CCM Call Mgr Status

Service Type: VoIP

Collection Method: SNMP

Instances on a Device: Single

Supported Platforms: Cisco® CallManager Version 4.1

Device Class: Windows Server

Monitoring Probe: Network Windows Probe, Workgroup Windows Probe, and WSP

Monitoring Probe Version: 4.5 SP1 and greater

The Cisco CallManager (CCM) Call Mgr Status service monitors the availability of the applications used to deliver a specific IP Telephony solution. These applications include the CallManager, Call Dispatcher, TFTP Service, and Messaging Interface.

The status provided by the service is an aggregated status of the availability of all of the applications.

Service Details

CCM Call Mgr Status Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Monitoring Probe	
Service Description	
Scan Interval	
ccmStatus Index	The index corresponding to the row in the ccmTable that contains the ccmStatus. The index is typically a value of 1 or 2, but can also be an integer.

Status Details

CCM Call Mgr Status Status Details

Status Detail	Description
Call Manager Status	The current status of the CallManager. The CallManager is available if the SNMP agent received a system up event from the local CCM.

Chapter 14

CCM Conf Activity

Service Type:	VoIP
Collection Method:	WMI
Instances on a Device:	Single
Supported Platforms:	Cisco® CallManager Version 4.1
Device Class:	Windows Server
Monitoring Probe:	Network Windows Probe, Workgroup Windows Probe, and WSP
Monitoring Probe Version:	4.5 SP1 and greater

The Cisco CallManager (CCM) Conf Activity service monitors the state of all of the conference hardware resources that are connected to the CallManager.

Service Details

CCM Conf Activity Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Service Description	
Scan Interval	

Status Details

CCM Conf Activity Status Details

Status Details	Description
Active Hardware Conferences	The total number of hardware conference devices that are currently registered with the CallManager and are in use (active).
Completed Hardware Conferences	The total number of hardware conferences on which conferences have been terminated.
Total Hardware Conference Resources	Available Hardware Conf Resources + Active Hardware Conferences
Available Hardware Conf Resources	The total number of hardware conference resources that are currently registered with the CallManager and are in use (active).

Status Details	Description
Active Hardware Conference Resources	The total number of hardware conference resources that are currently registered with the CallManager and are not in use (available).
Hardware Conf Resource Utilization (%)	A calculated percentage of the hardware conference resource utilization: Active Hardware Conferences * 100 / (Active Hardware Conference + Available Hardware Conf Resources)
Out of HW Conf Resources Incidents	The total number of attempts made to find a hardware conference resource when all other registered hardware conference resources were in use.

Chapter 15

CCM Conference Registration

Service Type:	VoIP
Collection Method:	SNMP
Instances on a Device:	Single
Supported Platforms:	Cisco® CallManager Version 4.1
Device Class:	Windows Server
Monitoring Probe:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, and WSP
Monitoring Probe Version:	4.5 SP1 and greater

The Cisco CallManager (CCM) Conference Registration service monitors the state of all of the conference media devices that are connected to the CallManager. This includes the media devices that have registered, unregistered, or attempted to register and been rejected with the CallManager.

Service Details

CCM Conference Registration Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Monitoring Probe	
Service Description	
Scan Interval	

Status Details

CCM Conference Registration Status Details

Status Detail	Description
Registered Media Devices	The total number of media devices that are present in the VoIP network, are active, and available for use.
Unregistered Media Devices	The total number of media devices that have been removed or have lost contact with the VoIP network.
Rejected Media Devices	The total number of media devices that have been configured incorrectly.

Chapter 16

CCM CTI Activity

Service Type:	VoIP
Collection Method:	WMI
Instances on a Device:	Single
Supported Platforms:	Cisco® CallManager Version 4.1
Device Class:	Windows Server
Monitoring Probe:	Network Windows Probe, Workgroup Windows Probe, and WSP
Monitoring Probe Version:	4.5 SP1 and greater

The Cisco CallManager (CCM) Computer Telephony Interface (CTI) Activity service monitors the state of the lines and devices that are connected to the CallManager.

Service Details

CCM CTI Activity Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Service Description	
Scan Interval	

Status Details

CCM CTI Activity Status Details

Status Detail	Description
CCM Links Active	The total number of links that are currently registered with the CallManager and are in use (active).
CTI Connections Active	The total number of links that are currently registered with the CallManager and are not in use (available).
Devices Open	The total number of devices—such as hardware IP phones, CTI ports, and CTI route points—that are connected to the CallManager and are controlled and/or monitored by CTI applications.
Links Open	The total number of links that are connected to the CallManager and are controlled and/or monitored by CTI applications.

Chapter 17

CCM CTI Registration

Service Type:	VoIP
Collection Method:	SNMP
Instances on a Device:	Single
Supported Platforms:	Cisco® CallManager Version 4.1
Device Class:	Windows Server
Monitoring Probe:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, and WSP
Monitoring Probe Version:	4.5 SP1 and greater

The Cisco CallManager (CCM) Computer Telephony Interface (CTI) Registration service monitors the state of the CTI devices that are connected to the CallManager. This includes the CTI devices that have been registered, unregistered, or have lost contact with the CallManager. In addition, the number of registration requests that have been rejected by the CallManager is also monitored by this service.

Service Details

CCM CTI Registration Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Monitoring Probe	
Service Description	
Scan Interval	

CCM CTI Registration Status Details

Status Detail	Description
Registered CTI Devices	The total number of CTI devices that are present in the VoIP network, are active, and available for use.
Unregistered CTI Devices	The total number of CTI devices that have been removed or have lost contact with the VoIP network.
Rejected CTI Devices	The total number of CTI devices that have been configured incorrectly.

Chapter 18

CCM Gateway Registration

Service Type:	VoIP
Collection Method:	SNMP
Instances on a Device:	Single
Supported Platforms:	Cisco® CallManager Version 4.1
Device Class:	Windows Server
Monitoring Probe:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, and WSP
Monitoring Probe Version:	4.5 SP1 and greater

The Cisco CallManager (CCM) Gateway Registration service monitors the state of the gateway devices that are connected to the CallManager. This includes the gateway devices that have registered, unregistered, or attempted to register and been rejected with the CallManager.

Service Details

CCM Gateway Registration Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Monitoring Probe	
Service Description	
Scan Interval	

Status Details

CCM Gateway Registration Status Details

Status Detail	Description
Registered Gateways	The total number of registered gateways that are registered with the CallManager.
Unregistered Gateways	The total number of unregistered gateways that have been removed or have lost contact with the VoIP network.
Rejected Gateways	The total number of gateways that have been configured incorrectly.

Chapter 19

CCM ISDN - T1 Trunks

Service Type: VoIP

Collection Method: WMI

Instances on a Device: Single

Supported Platforms: Cisco® CallManager Version 4.1

Device Class: Windows Server

Monitoring Probe: Network Windows Probe, Workgroup Windows Probe, and WSP

Monitoring Probe Version: 4.5 SP1 and greater

The Cisco CallManager (CCM) ISDN - T1 Trunks service monitors the utilization of T1 trunks, the ISDN Basic Rate Interface, and Primary Rate Interface (BRI/PRI) trunks.

Service Details

CCM ISDN - T1 Trunks Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Service Description	
Scan Interval	

Status Details

CCM ISDN - T1 Trunks Status Details

Status Detail	Description
Active PRI Voice Channels	The number of active calls on the PRI trunk.
PRI Spans in Service	The number of available PRI trunk spans.
PRI Utilization (%)	A calculated percentage of the PRI utilization: Active PRI Voice Channels * 100 / PRI Spans in Service * 23
Active T1 CAS Voice Channels	The number of active calls on the T1 trunk.
T1 CAS Spans in Service	The number of available T1 trunk spans.

Status Detail	Description
T1 Utilization (%)	A calculated percentage of the T1 utilization: Active T1 CAS Voice Channels * 100 / T1 CAS Spans in Service * 24
Active BRI Voice Channels	The number of active calls on the BRI trunk.
BRI Spans in Service	The number of available BRI trunk spans.
BRI Utilization (%)	A calculated percentage of the BRI utilization: Active BRI Voice Channels * 100 / BRI Spans in Service * 2

Chapter 20

CCM MTP - Transcoder

Service Type:	VoIP
Collection Method:	WMI
Instances on a Device:	Single
Supported Platforms:	Cisco® CallManager Version 4.1
Device Class:	Windows Server
Monitoring Probe:	Network Windows Probe, Workgroup Windows Probe, and WSP
Monitoring Probe Version:	4.5 SP1 and greater

The Cisco CallManager (CCM) Media Termination Point (MTP) - Transcoder service monitors the state of the transcoder resources that are available to the CallManager.

Service Details

CCM MTP - Transcoder Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Service Description	
Scan Interval	

Status Details

CCM MTP - Transcoder Status Details

Status Detail	Description
Total MTP Resources	The total of active and available MTP resources: Active MTP Resources + Available MTP Resources
Active MTP Resources	The total number of MTP resources that are currently registered with the CallManager and are in use (active).
Available MTP Resources	The total number of MTP resources that are currently registered with the CallManager and are not in use (available).

Status Detail	Description
MTP Resource Utilization (%)	A calculated percentage of the MTP resource utilization: Active MTP Resources * 100 / (Active MTP Resources + Available MTP Resources)
MTP Out of Resources Incidents	The total number of attempts made to find an MTP resource when all other registered MTP resources were in use.
Total Transcoder Resources	The total number of active and available transcoder resources: Active Transcoder Resources + Available Transcoder Resources
Active Transcoder Resources	The total number of transcoder resources that are currently registered with the CallManager and are in use (active).
Available Transcoder Resources	The total number of transcoder resources that are currently registered with the CallManager and are not in use (available).
Transcoder Resource Utilization (%)	A calculated percentage of the transcoder resource utilization: Active Transcoder Resources * 100 / (Active Transcoder Resources + Available Transcoder Resources)
Transcoder Out of Resources Incidents	The total number of attempts made to find a transcoder resources when all other registered MTP resources were in use.

Chapter 21

CCM Music on Hold

Service Type: VoIP

Collection Method: WMI

Instances on a Device: Single

Supported Platforms: Cisco® CallManager Version 4.1

Device Class: Windows Server

Monitoring Probe: Network Windows Probe, Workgroup Windows Probe, and WSP

Monitoring Probe Version: 4.5 SP1 and greater

The Cisco CallManager (CCM) Music on Hold (MoH) service monitors the state of the MoH resources that are connected to the CallManager.

Service Details

CCM Music on Hold Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Service Description	
Scan Interval	

Status Details

CCM Music on Hold Status Details

Status Detail	Description
Total Multicast Resources	The total number of MoH multicast resources that are currently registered with the CallManager.
Active Multicast Resources	The total number of MoH multicast resources that are currently registered with the CallManager and are in use (active).
Available Multicast Resources	The total number of MoH multicast resources that are currently registered with the CallManager and are not in use (available).
Multicast Resource Utilization (%)	A calculated percentage of the multicast resource utilization: Active Multicast Resources * 100 / Total Multicast Resources

Status Detail	Description
Out of Resources	The total number of attempts made to find an MoH resource when all other registered MoH resources were in use.
Total Unicast Resources	The total number of unicast MoH resources that are registered with the CallManager.
Active Unicast Resources	The total number of unicast MoH resources that are currently registered with the CallManager and are in use (active).
Available Unicast Resources	The total number of unicast MoH resources that are currently registered with the CallManager and are not in use (available).
Unicast Resource Utilization (%)	A calculated percentage of the unicast resource utilization: Active Unicast Resource * 100 / Total Unicast Resources

Chapter 22
CCM Performance

Service Type: VoIP
Collection Method: WMI
Instances on a Device: Single
Supported Platforms: Cisco® CallManager Version 4.1
Device Class: Windows Server
Monitoring Probe: Network Windows Probe, Workgroup Windows Probe, and WSP
Monitoring Probe Version: 4.5 SP1 and greater

The Cisco CallManager (CCM) Performance service monitors key performance indicators on the CallManager. This includes:

- the average expected delay before calls are answered;
- the number of calls rejected due to call throttling; and
- metrics on code entry and exit conditions.

Service Details

CCM Performance Service Details

Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Service Description	
Scan Interval	

Status Details

CCM Performance Status Details

Status Detail	Description
Average Expected Delay (ms)	The CallManager's delay in responding to the calls.
Calls rejected due to call throttling	The Number of calls rejected due to call throttling.
Code Red Entry and Exit	The number of times the CallManager fails.
Code Yellow Entry and Exit	The number of warnings that are displayed before CallManager failure.

Chapter 23

CCM Phone Registration

Service Type:	VoIP
Collection Method:	SNMP
Instances on a Device:	Single
Supported Platforms:	Cisco® CallManager Version 4.1
Device Class:	Windows Server
Monitoring Probe:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, and WSP
Monitoring Probe Version:	4.5 SP1 and greater

The Cisco CallManager (CCM) Phone Registration service monitors the presence of the telephone instruments that are connected to the CallManager. This includes the telephone instruments that have been registered, unregistered, or have lost contact with the CallManager. In addition, the number of registration requests that have been rejected by the CallManager is also monitored by this service.

Service Details

CCM Phone Registration Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Monitoring Probe	
Service Description	
Scan Interval	

Status Details

CCM Phone Registration Status Details

Status Detail	Description
Registered Phones	The telephone instruments that are present in the VoIP network, active, and available for use.

Status Detail	Description
Unregistered Phones	The telephone instruments that have been removed or have lost contact with the VoIP network.
Rejected Phones	The telephone instruments that have been configured incorrectly.

Chapter 24

CCM Server

Service Type:	VoIP
Collection Method:	WMI
Instances on a Device:	Single
Supported Platforms:	Cisco® CallManager Version 4.1
Device Class:	Windows Server
Monitoring Probe:	Network Windows Probe, Workgroup Windows Probe, and WSP
Monitoring Probe Version:	4.5 SP1 and greater

The Cisco CallManager (CCM) Server service monitors the server on which the Cisco CallManager application is installed. The service merges the CPU (WMI), Disk (WMI), and Memory (WMI) services and monitors the CPU, Disk, and Memory utilization of the CallManager through one task.

If there are multiple CPUs, an average of the CPU utilization is calculated and, similarly, if there are multiple disks, an average Disk utilization is calculated. There is only one memory pool on the x86 platform, therefore, an average of the memory utilization does not need to be calculated.

If you would like to monitor a specific CPU or disk, set the CPU (WMI) or Disk (WMI) service on the CallManager. For more information, refer to CPU on page 83 or Disk on page 91.

Service Details

CCM Server Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Service Description	
Scan Interval	

Status Details

CCM Server Status Details

Status Detail	Description
CPU Utilization (%)	A calculated percentage of the CPU utilization: Sum of Processor.LoadPercentage / Count of Processor Objects
Free Disk Space (KB)	A calculated percentage of the free disk space utilization: Sum of LogicalDisk.FreeSpace / 1000
Disk Utilization (%)	A calculated percentage of the disk utilization: (Sum of LogicalDisk.Size - Sum of LogicalDisk.FreeSpace) * 100 / Sum of LogicalDisk.Size
Physical Memory Utilization (%)	A calculated percentage of the physical memory utilization: (OperatingSystem.TotalVisibleMemorySize - OperatingSystem.FreePhysicalMemory) * 100 / OperatingSystem.TotalVisibleMemorySize
Virtual Memory Utilization (%)	A calculated percentage of the virtual memory utilization: (OperatingSystem.TotalVirtualMemorySize - OperatingSystem.FreeVirtualMemory) * 100 / OperatingSystem.TotalVirtualMemorySize

Chapter 25

CCM VoiceMail Registration

Service Type:	VoIP
Collection Method:	SNMP
Instances on a Device:	Single
Supported Platforms:	Cisco® CallManager Version 4.1
Device Class:	Windows Server
Monitoring Probe:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, and WSP
Monitoring Probe Version:	4.5 SP1 and greater

The Cisco CallManager (CCM) VoiceMail Registration service monitors the presence of the voice mail devices that are connected to the CallManager. This includes voice mail devices that have been registered, unregistered, or have lost contact with the CallManager. In addition, the number of registration requests that have been rejected by the CallManager is also monitored by this service.

Service Details

CCM VoiceMail Registration Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Monitoring Probe	
Service Description	
Scan Interval	

Status Details

CCM VoiceMail Registration Status Details

Status Detail	Description
Registered Voice Mail Devices	The voice mail devices that are present in the VoIP network, are active, and available for use.

Status Detail	Description
Unregistered Voice Mail Devices	The voice mail devices that have been removed or have lost contact with the VoIP network.
Rejected Voice Mail Devices	The voice mail devices that have been configured incorrectly.

Chapter 26

Citrix® Presentation Server

Service Type:	Network
Collection Method:	Generic TCP
Instances on a Device:	Multiple (up to 3 instances)
Supported Platforms:	Citrix® MetaFrame® Presentation
Device Class:	Generic Server, Generic Workstation, Novell, Other, Printer, Scanner/ Camera, Switch/Router, Windows Server, and Windows Workstation
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, Central Server
Service Version:	N-central 4.5 and greater

The Citrix Presentation Server service monitors the availability of the port on which the Citrix Metaframe Presentation Server application runs. The availability of the port, which is determined by the service testing the port's connectivity, indicates that the Citrix Metaframe Presentation Server application is running. This service also measures the domain name system (DNS) resolution and the round trip time of the initial connection request and response. The availability results of the TCP service are then reflected on the status dashboard for the Citrix Presentation Server service.

A maximum of three instances of this service can be set on a device, with each instance monitoring a different port on the device.

The Citrix Presentation Server service does not use the Warning state.

Service Details

Citrix Presentation Server Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Timeout Value	
Port Number	

Status Details

Citrix Presentation Server Status Details

Status Detail	Description
Citrix Presentation Server service Availability	The threshold that determines the availability of the port.
Average Round Trip Time (ms)	The time (in milliseconds) for a request to be sent and received.
Generic DNS Resolution	The threshold that determines whether the device name can be resolved. If an FQDN has been specified, the service searches for its IP address. If the IP address is found, the state will be Normal. Otherwise, it will be Failed, based on the default settings. If an IP address has been specified, the service checks only the IP address's format. If the format is correct, the state will be Normal. Otherwise, it will be Failed, based on the default settings.

Chapter 27

Connectivity

Service Type:	Network
Collection Method:	TCP/ICMP
Instances on a Device:	Single
Supported Platforms:	N/A
Device Class:	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server
Service Version:	N-central 3.0 and greater

N-central can monitor a network device for connectivity to the network. The connectivity test ensures that the monitored device is participating in the network and is ready to accept connections.

The connectivity test uses the Internet Control Message Protocol (ICMP) to test the availability of this service. N-central sends ICMP packets to the targeted network device. The connectivity test can determine the quality of the connection, compare the quality of the connection to the defined thresholds, and return a status level.

Warning! The connectivity service may not function properly when monitored by probes installed on systems using Windows Vista. This is due to the default setting in Windows Firewall with Advanced Security that does not allow incoming ICMP Echo messages. This may be resolved by enabling ICMP Echo messages through the creation of new inbound custom rules to allow ICMPv4 and ICMPv6 Echo Requests. For more information, refer to Microsoft documentation on Windows Firewall with Advanced Security.

Service Details

Connectivity Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Timeout Value	
Packet Interval	The time (in seconds) between packets.
Packet Number	The number of packets to send for each scan.
Packet Size	The number of data bytes in each packet.
Default TTL	Time to live (TTL), which is the number of hops that a data packet must take before being discarded or returned. A hop is the trip that a data packet takes from one router to the next in a network. As each router receives the packet, it subtracts one from the TTL count. The data packet carries the new TTL count in its header to the next router. When the count reaches zero, the router that detects the zero value, discards the packet and sends an ICMP message about the transmission failure back to the originator. A transmission failure occurs if the TTL count does not match the actual number of hops configured in the network.

Status Details

Connectivity Status Details

Status Details	Description
Packet Loss (percentage)	A packet is dropped when its TTL value reaches zero or when the remote host is unreachable. When a packet is dropped, the echoed packet is never received.
Time to Live (hops)	A state transition for the service occurs when the threshold value exceeds the specified range for any of these threshold types.
Round Trip Time (ms)	The time (in milliseconds) for a request to be sent and received.
DNS Resolution	The threshold that determines whether the device name can be resolved. If an FQDN has been specified, the service searches for its IP address. If the IP address is found, the state will be Normal. Otherwise, it will be Failed, based on the default settings. If an IP address has been specified, the service checks only the IP address's format. If the format is correct, the state will be Normal. Otherwise, it will be Failed, based on the default settings.

Chapter 28
CPU

A CPU service monitors the use of the central processing unit (CPU) of a device.

Table 28-1 summarizes the CPU services available through N-central and what they monitor.

Table 28-1: CPU Services and What They Monitor

CPU Service	Monitors
CPU (Local API)	Average CPU usage over the last scan interval.
CPU (SNMP)	Average CPU usage over the last minute.
CPU (WMI)	Average CPU usage over the last second.
CPU (Cisco)	CPU usage by any SNMP CISCO-PROCESS-MIB Compliant Device.

CPU Services (Local API, SNMP, WMI)

Service Type:	System
Collection Method:	Local API, SNMP, and WMI Workstation
Instances on a Device:	Multiple
Supported Platforms:	Agent and HOST-RES Compliant SNMP devices
Device Class for CPU (Local API):	Generic Server, Generic Workstation, Windows Server, and Windows Workstation
Device Class for CPU (SNMP):	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Device Class for CPU (WMI):	Windows Server and Windows Workstation
Monitored By:	Agent (Windows, Novell Netware, RedHat Linux, RedHat Enterprise Linux, Suse Linux, and Mac OSX 10.4)
Service Version:	N-central 3.0 and greater

Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to

Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2 published by Microsoft®.

Service Details

CPU (Local API, SNMP, WMI) Common Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	

CPU (Local API) Service Details

Service Detail	Description
Processor Number	The ID number of the processor that you would like to monitor.

CPU (SNMP) Service Details

Service Detail	Description
Processor Index	The index of the processor to monitor.

Configuring Processor Index for CPU (SNMP)

To configure Processor Index

To obtain the processor index, walk the object ID .1.3.6.1.2.1.25.3.3.1.2 on the target device's address to determine which indices are available for monitoring.

Example:

```
.1.3.6.1.2.1.25.3.3.1.2.1 50
.1.3.6.1.2.1.25.3.3.1.2.2 10
```

Substituting the numerical object ids with their textual representations, the walk becomes:

```
hrProcessorLoad.1 50
hrProcessorLoad.2 10
```

There are two indices in this case—"1" and "2".

To monitor both processors, add the service to the device and enter “1” for the Processor Index. Add the service a second time and enter “2” for the Processor Index.

WMI CPU Service Details

Service Detail	Description
Processor Name	A unique identifier, which represents the processor.

Configuring Processor Name for WMI CPU

Use the Web Based Enterprise Management (wbemtest) tool in Windows to get the Processor Name service detail.

To configure Processor Name

1. Press the Windows Explorer key + R.
   ↳ The Run dialog box appears.
2. Specify wbemtest in the Open field, and press Enter.
   ↳ The Windows Management Instrumentation Tester dialog box appears.
3. Click Connect.
   ↳ The Connect dialog box appears.
4. In the first field, specify the namespace: \\<your host name>\root\cimv2.
5. Click Connect.
   ↳ The Windows Management Instrumentation Tester dialog box appears, with the namespace you have specified.
6. Click Enum Instances.
   ↳ The Class Info dialog box appears.
7. In the Enter superclass name field, specify: Win32_Processor.
8. Click OK.
   ↳ The Query Results dialog box appears. It should list at least one line, for example: "Win32_Processor.DeviceID="CPU0". The Processor Name service detail includes the quotations and the value within the quotations. In this example, the Processor Name service detail is “CPU0”.

Status Details

CPU (Local API, SNMP, WMI) Status Details

Status Detail	Description
CPU Usage (%)	The amount of CPU usage that is compared to the threshold values. The amount is calculated as a percentage.

CPU (Cisco)

Service Type: System

Collection Method: SNMP

Instances on a Device: Multiple

Supported Platforms: Any Cisco equipment that supports CISCO-PROCESS-MIB

Device Class for CPU (SNMP): Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Hardware Probe, Windows Probes

Service Version: N-central and greater

Service Details

CPU (Cisco) Service Details

Service Detail	Description
Monitoring	Refer to .
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	
CPU Index	The index of the location name of the power supply, which is determined by performing an SNMP walk on cpmCPUTotal5sec (.1.3.6.1.4.1.9.9.109.1.1.1.1.3).

Configuring CPU Index for CPU (Cisco)

Permission Levels: Product Admin, SO Admin, SO Tech, and Admin

To configure CPU Index

To obtain the processor index for CPU, walk the OID .1.3.6.1.4.1.9.9.109.1.1.1 on the target device's SNMP agent to determine which indices are available for monitoring.

Example:

```
.1.3.6.1.4.1.9.9.109.1.1.1.1.3.0 90
.1.3.6.1.4.1.9.9.109.1.1.1.1.3.1 50
.1.3.6.1.4.1.9.9.109.1.1.1.1.4.0 70
.1.3.6.1.4.1.9.9.109.1.1.1.1.4.1 30
.1.3.6.1.4.1.9.9.109.1.1.1.1.5.0 50
.1.3.6.1.4.1.9.9.109.1.1.1.1.5.1 10
```

Substituting the numerical object ids with their textual representations, the walk becomes:

```
cpmCPUTotal5sec.0 90
cpmCPUTotal5sec.1 50
cpmCPUTotal1min.0 70
cpmCPUTotal1min.1 30
cpmCPUTotal5min.0 50
cpmCPUTotal5min.1 10
```

There are two indices in this case—"0" and "1". To monitor both processors, add the service and enter “0” for the CPU Index; then add the service again and enter “1” for the CPU Index.

Status Details

CPU (Cisco) Status Details

Status Detail	Description
% CPU Utilization (5 Seconds)	The overall CPU busy percentage for the last 5 second period.
% CPU Utilization (1 Minute)	The overall CPU busy percentage for the last 1 minute period.
% CPU Utilization (5 Minutes)	The overall CPU busy percentage for the last 5 minute period.

Chapter 29

Device Status

Service Type:	System
Collection Method:	SNMP
Instances on a Device:	Multiple
Supported Platforms:	Any SNMP HOST-RESOURCES-MIB Compliant Device (RFC1514)
Device Class:	Windows Server, Generic Server, Printer, Scanner/Camera, Switch/Router, and Other
Monitored By:	Hardware Probe
Service Version:	N-central 5.1 and greater

The Device Status service monitors the current operational state of a device and reports a description including the device's manufacturer and revision value.

Note: Optionally, this service may also report the device's serial number.

Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	

Configuring Device Status

Walk the OIDs on the target device's SNMP agent to determine which indices are available for monitoring.

Example:

```
.1.3.6.1.2.1.25.3.2.1.3.1 "hp LaserJet 4200"
.1.3.6.1.2.1.25.3.2.1.3.2 "Hewlett-Packard Dynamic RAM Disk"
.1.3.6.1.2.1.25.3.2.1.5.1 3
.1.3.6.1.2.1.25.3.2.1.5.2 2
```

Substituting the OIDs with the MIBs the walk becomes:

```
hrDeviceDescr.1  "hp LaserJet 4200"
hrDeviceDescr.2  "Hewlett-Packard Dynamic RAM Disk"
hrDeviceStatus.1 3
hrDeviceStatus.2 2
```

There are two indices in this case - "1" and "2".

Device Status #1

```
Device Description Instance ID = "1"
Device Status Instance ID      = "1"
```

Device Status #2

```
Device Description Instance ID = "2"
Device Status Instance ID      = "2"
```

Status Details

Status Detail	Description
Device Status	The current operational state of the device indicated as either: • **Unknown** - the current state of the device is unknown. • **Running** - the device is up and running and that no unusual error conditions are known. • **Warning** - the agent has been informed of an unusual error condition by the operational software (for example, a disk device driver) but that the device is still operational. • **Testing** - the device is not available for use because it is currently in the testing state. • **Down** - used only when the agent has been informed that the device is not available for any use.
Device Description	The device name obtained by SNMP.

Chapter 30
Disk

Service Type:	System
Collection Method:	Local API, SNMP, and WMI Workstation
Instances on a Device:	Multiple
Supported Platforms:	N/A
Device Class for Disk (Local API):	Generic Server, Generic Workstation, Windows Server, and Windows Workstation
Device Class for Disk (SNMP):	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Device Class for Disk (WMI):	Windows Server and Windows Workstation
Monitored By:	Agent (Windows, Novell Netware, RedHat Linux, RedHat Enterprise Linux, SUSE Linux, and Mac OSX 10.4), SNMP (Network Hardware Probe), and WMI (Windows probes)
Service Version:	N-central 3.0 and greater

Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* published by Microsoft®.

The Disk service monitors a partition of a hard disk for its used, free, and total disk space. A maximum of 10 partitions on a device can be monitored by this service. The Disk service must be added on each partition and set up before monitoring can begin. The results are displayed on the status dashboard under the service and, if specified, can also be provided in any notifications triggered by the service.

Service Details

Disk Common Service Details

Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	

Local API and WMI Service Details

Detail	Description
Volume Name	The name of the hard disk or partition to monitor.

SNMP Service Details

Detail	Description
Volume Name	The name of the hard disk or partition to monitor.
Volume Index	The index of the SNMP object representing the partition of hard disk to monitor.

Configuring Volume Name or Volume Index

Walk the object ID .1.3.6.1.2.1.25.2.3 on the target device's address to determine which indices are available for monitoring.

Example:

```
 .1.3.6.1.2.1.25.2.3.1.3.1 "A:\"
 .1.3.6.1.2.1.25.2.3.1.3.2 "C:\ Label:  Serial Number 74ebc3fb"
 .1.3.6.1.2.1.25.2.3.1.3.3 "D:\ Label:SP2POEM_EN  Serial Number
356563d9"
 .1.3.6.1.2.1.25.2.3.1.3.4 "Virtual Memory"
 .1.3.6.1.2.1.25.2.3.1.4.1 0
 .1.3.6.1.2.1.25.2.3.1.4.2 4096
 .1.3.6.1.2.1.25.2.3.1.4.3 2048
 .1.3.6.1.2.1.25.2.3.1.4.4 65536
 .1.3.6.1.2.1.25.2.3.1.5.1 0
 .1.3.6.1.2.1.25.2.3.1.5.2 19535032
 .1.3.6.1.2.1.25.2.3.1.5.3 188358
 .1.3.6.1.2.1.25.2.3.1.5.4 44119
 .1.3.6.1.2.1.25.2.3.1.6.1 0
 .1.3.6.1.2.1.25.2.3.1.6.2 985599
 .1.3.6.1.2.1.25.2.3.1.6.3 188358
 .1.3.6.1.2.1.25.2.3.1.6.4 0
```

Substituting the numerical object Ids with their textual representations, the walk becomes:

```
 hrStorageDescr.1           "A:\"
 hrStorageDescr.2           "C:\ Label:  Serial Number 74ebc3fb"
 hrStorageDescr.3           "D:\ Label:SP2POEM_EN  Serial Number
356563d9"
 hrStorageDescr.4           "Virtual Memory"
 hrStorageAllocationUnits.1 0
 hrStorageAllocationUnits.2 4096
 hrStorageAllocationUnits.3 2048
 hrStorageAllocationUnits.4 65536
 hrStorageSize.1            0
 hrStorageSize.2            19535032
 hrStorageSize.3            188358
 hrStorageSize.4            44119
 hrStorageUsed.1            0
 hrStorageUsed.2            985599
 hrStorageUsed.3            188358
 hrStorageUsed.4            0
```

Status Details

Status Details

Status Detail	Description
Total Disk Size (KB)	The total partition or disk capacity, expressed in kilobytes.
Disk Space Used (KB)	The total occupied space on the partition or disk, expressed in kilobytes.
Disk Free Space (KB)	The unoccupied space on the partition or disk, expressed in kilobytes.
Disk Usage (%)	The calculated capacity utilization of the partition or disk, expressed as a percentage.

Chapter 31

Disk Queue Length

Service Type:	System
Collection Method:	WMI Station
Instances on a Device:	Multiple
Supported Platforms:	Any WMI-enabled Windows server or workstation
Device Class:	Windows Server, Windows Workstation
Monitored By:	Windows Probes
Service Version:	N-central 5.0 and greater

Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* published by Microsoft®.

The Disk Queue Length service monitors the number of read and write requests outstanding on the disk.

Service Details

Disk Queue Length Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	
Instance	An instance of the WMI class Win32_PerfRawData_PerDisk_PhysicalDisk; for example, “_Total”. To find the disk name to monitor, start Perfmon in Windows. Then click the Add Counters button and in the Performance Object drop down choose "Physical Disk". The available instances display in the right hand window under "Select instances from list:". For Disk Constraint, enter the value contained within the quotations. You must specify a WSP probe as the monitoring endpoint since this is a WMI service. The device class of the device must be Windows Server or Windows Workstation.

Status Details

Disk Queue Length Status Details

Status Detail	Description
Current Queue	Number of requests outstanding on the disk at the time the performance data is collected, including requests in service at the time of the snapshot. The value represents an instantaneous length, not an average over a time interval. Multi-spindle disk devices can have multiple requests active at one time, but other concurrent requests await service. This property may reflect a transitory high or low queue length. If the disk drive has a sustained load, the value will be consistently high. Requests experience delays proportional to the length of the queue minus the number of spindles on the disks. This difference should average less than 2 for good performance.
Average Queue	Average number of both read and write requests that were queued for the selected disk during the sample interval.

Chapter 32
DNS

Service Type:	Network
Collection Method:	TCP/UDP
Instances on a Device:	Single
Supported Platforms:	N/A
Device Class:	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server
Service Version:	N-central 3.0 and greater

The DNS service monitors the domain name system (DNS) server for its availability. The results from monitoring are displayed on the status dashboard under the service and, if specified, can also be provided in any notifications triggered by the service.

During the monitoring process, a name server lookup (nslookup) is run at the preset scan intervals to test the availability of the DNS server. If the DNS server returns all of the IP addresses of the specified FQDN, the test is successful.

The nslookup is run using the user datagram protocol (UDP). If a DNS response to the DNS query is too large for the UDP packet, then the service state is displayed as Failed, although the DNS server is functional. For this reason, to receive accurate results of the DNS server's availability, specify an FQDN that will return fewer IP addresses for the FQDN to Resolve service detail. An FQDN that returns fewer IP addresses has a greater chance of fitting into the UDP packet.

The DNS service can monitor the DNS server through the central server, a Windows probe, or a Network Hardware probe. If the DNS server is on a public network, the central server is used. If the DNS server is on a private network, a probe is used to send the information received from the DNS server through the firewall to the central server.

Figure 32-1 and Figure 32-2 display the monitoring processes of the DNS server on a private and public network.

Figure 32-1: Monitoring the DNS Server on a Private Network

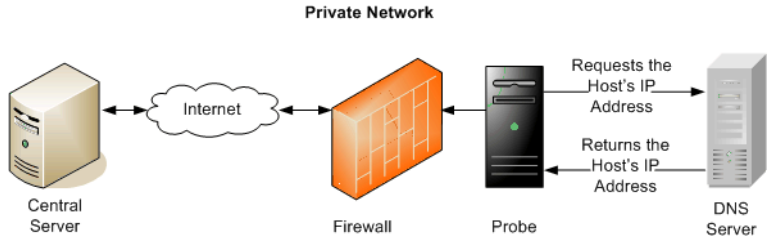
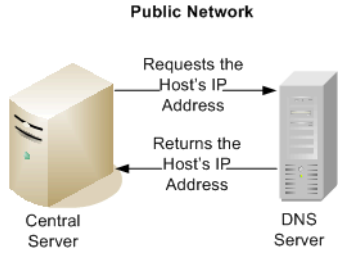


Figure 32-2: Monitoring the DNS Server on a Public Network



To monitor the DNS server, you must:

- Add the DNS server as a device. For more information, refer to Adding Devices in the *Customer Manual*.
- Add the DNS service to the device. For more information, refer to Adding Services in the *Customer Manual*.

Service Details

DNS Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Timeout Value	
Port Number	
FQDN to Resolve	The resolvable fully qualified domain name (FQDN) used to determine service availability.

Status Details

DNS Status Details

Status Detail	Description
DNS Service Availability	Determines whether the DNS service is up or down. The DNS service does not use the Warning state. For example, a DNS test is considered successful if the target DNS server is able to resolve www.<Web site name>.com.
Round Trip Time (ms)	The time (in milliseconds) for a request to be sent and received.
DNS Resolution	The threshold that determines whether the device name can be resolved. If an FQDN has been specified, the service searches for its IP address. If the IP address is found, the state will be Normal. Otherwise, it will be Failed, based on the default settings. If an IP address has been specified, the service checks only the IP address's format. If the format is correct, the state will be Normal. Otherwise, it will be Failed, based on the default settings.

Chapter 33

Ethernet Errors

Service Type:	Network
Collection Method:	SNMP
Instances on a Device:	Multiple
Supported Platforms:	N/A
Device Class:	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe
Service Version:	N-central 3.5 and greater

Ethernet is a type of networking technology that is used to transmit data within local area networks (LANs). It is commonly used to transmit local area network (LAN) traffic quickly.

Unlike connection oriented networking protocols that establish (virtual) circuits between target systems, Ethernet is a media that is shared among a varied number of hosts. This can result in different types of errors when there are a lot of systems that are trying to use the media simultaneously.

N-central can monitor different types of counters associated with errors detected when transmitting and receiving packets on Ethernet interfaces. Based on the values of these counters, N-central can determine if congestion is present on the network.

To monitor the Ethernet Errors service on a device, you must:

- Select the SNMP Enabled option when adding the device. For more information, refer to Adding Devices in the *Customer Manual*.
- Run interface discovery on the device. For more information, refer to Discovering Interfaces for SNMP Services in the *Customer Manual*.
- Add the Ethernet Errors service to the device. For more information, refer to Adding Services in the *Customer Manual*.
- After interface discovery is complete, set the Interfaces to Monitor service detail for the Ethernet Errors service. For more information, refer to Setting Interfaces for SNMP Services in the *Customer Manual*.

The tables IF-MIB and EtherLike-MIB describe the SNMP objects that are queried by the probe.

IF-MIB

Object Descriptors	Numerical OID
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2

EtherLike-MIB

Object Descriptors	Numerical OID
dot3StatsIndex	1.3.6.1.2.1.10.7.2.1.1
dot3StatsAlignmentErrors	1.3.6.1.2.1.10.7.2.1.2
dot3StatsFCSErrors	1.3.6.1.2.1.10.7.2.1.3
dot3StatsSingleCollisionFrames	1.3.6.1.2.1.10.7.2.1.4
dot3StatsMultipleCollisionFrames	1.3.6.1.2.1.10.7.2.1.5
dot3StatsInternalMacReceiveErrors	1.3.6.1.2.1.10.7.2.1.16
dot3StatsInternalMacTransmitErrors	1.3.6.1.2.1.10.7.2.1.10
dot3StatsCarrierSenseErrors	1.3.6.1.2.1.10.7.2.1.11
dot3StatsFrameTooLongs	1.3.6.1.2.1.10.7.2.1.13

Service Details

Ethernet Errors Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Interfaces to Monitor	Displays the discovered names of the data items, such as port numbers and device names. This field is blank until interface discovery has been run.
Scan Interval	Refer to Table 1-1 on page 2.

Status Details

Ethernet Errors Thresholds

Status Details	Description
Thresholds	N-central applies the threshold metrics based on the interface. N-central determines the monitored data against the specified threshold values.
Alignment Errors	An Alignment Error can indicate the following about a received packet: • The number of bits in the received packet has an uneven byte count (not an integral multiple of 8). • The received packet has a Frame Check Sequence (FCS) error. • Alignment Errors often result from MAC layer packet formation problems and cabling problems. These problems cause corruption of data, loss in data and the transmission of packets through more than two cascaded multi-port transceivers.

Status Details	Description
FCS Errors	The Frame Check Sequence (FCS) is a mathematical way to ensure that all of the packet's bits are correct and saves N-central from having to examine each bit and compare it to the original. Packets with Alignment Errors also generate FCS Errors. FCS Errors, a type of cyclic redundancy checking, indicate that frames received by an interface are an integral number of octets long, but do not pass the FCS check. Both Alignment Errors and FCS Errors can be caused by equipment powering up or down or by noise interference on unshielded twisted-pair (10BASE-T) segments. In a network that complies with the Ethernet standard, FCS Errors or Alignment Errors indicate bit errors during a transmission or reception. A very low rate is acceptable. Although Ethernet allows a 1 in 108 bit error rate, typical Ethernet performance is 1 in 1012 or better.
Collisions	Collisions indicate that two or more devices detect that the network is idle and try to send packets at exactly the same time (within one round-trip delay). Because only one device can transmit at a time, both devices must stop sending and attempt to retransmit. Collisions are detected by the transmitting stations. The retransmission algorithm helps to ensure that the packets do not retransmit at the same time. However, if the devices retry at nearly the same time, packets can collide again; the process repeats until either the packets finally pass onto the network without collisions, or 16 consecutive collisions occur and the packets are discarded.
MAC Receive Errors	MAC receive errors can indicate the malfunction of an ethernet card on the subnet. You can identify the subnet and possibly the unit in question from the MAC address and the IP number. To obtain the name of the unit, you can use “arp”.
MAC Send Errors	This type of error indicates that the transmission failed because of an internal MAC sublayer error that is not caused by a collision or a carrier sense error.
Carrier Sense Errors	Indicates that the transmission failed because the carrier was not present during any or all of the transmission attempts.
Frame Too Long	A packet that is longer than 1518 octets (including FCS octets) can cause a: Frames Too Long Error. This type of error is often caused by a malfunction in the jabber protection mechanism on a transceiver, or the presence of excessive noise on the transmission cable. The threshold value units are measured in packets.

Chapter 34

Event Log

Service Type:	System
Collection Method:	Local API
Instances on a Device:	Multiple
Supported Platforms:	N/A
Device Class:	Generic Server, Generic Workstation, Windows Server, and Windows Workstation
Monitored By:	Agent (Windows)
Service Version:	N-central 3.0 and greater

The Event Log service allows you to monitor the logs that are managed by the Windows Event Viewer. This service displays the appropriate status for each instance of an event. You can view the status of the Event Log service on the status screen for the device details or service details, or by generating a Raw Monitored Data log report.

The Windows Event Viewer can manage the following six types of logs on a computer:

- Security,
- Application,
- System Log,
- Directory Service Log (only available on the Windows 2000 Server and Windows 2003 Server),
- File Replication Service Log (only available on the Windows 2000 Server and Windows 2003 Server), and
- DNS Server Log (only available on the Windows 2000 Server and Windows 2003 Server).

The options for the Directory Service, File Replication Service, and DNS Server logs are displayed only if the corresponding applications are installed on the computer.

The Event Viewer generates five event types for the logs listed above. The table Event Types of the Windows Event Viewer describes these events.

Event Types of the Windows Event Viewer

Event Type	Description
Error	Generates due to a loss of data or functionality.
Warning	Generates to indicate a problem that can occur in the future.

Event Type	Description
Information	Generates when the computer has successfully completed an operation.
Success	Generates when a secure domain can be accessed.
Failure	Generates when a secure domain cannot be accessed.

Only certain types of events can be tracked for each log. Each log and its associated event types are displayed on the Event Log configuration screen.The table Event Logs and Associated Event Types describes the event types that can be tracked for each log.

Event Logs and Associated Event Types

Event Log	Event Type
Security	Failure or Success
Application	Error, Information, or Warning
System log	Error, Information, or Warning
DNS Server	Error, Information, or Warning
File Replication Service	Error, Information, or Warning
Directory Service	Error, Information, or Warning

The event IDs that you would like to include or exclude during the monitoring process, can be specified individually or as a range. These IDs can be obtained from the Event column of the Event Viewer or from the Information Properties dialog of the selected event row. Whether you are specifying the event IDs individually or as a range, you must use the comma separated values (CSV) format and list them without any spaces. For a range of Event IDs, you can use a dash (-).

Each event that N-central processes for state can be up to 480 KB in size.

N-central sends a notification when a log generates the Failed state. After the notification is sent, N-central resets the Event Log service to the Normal state and, therefore, is ready to send another notification if another Failed state occurs.

Service Details

Event Log Service Details

Service Detail	Description
Options to Monitor: Security—Failure, Success Application—Error, Information, Warning System—Error, Information, Warning Directory Service—Error, Information, Warning File Replication Service—Error, Information, Warning DNS Server—Error, Information, Warning	The names of the Windows Event Viewer log that are to be monitored.
Include List	The event IDs that you would like to monitor. You can specify individual event IDs or a range of event IDs using the comma separated value (CSV) format, without any spaces. For example: 100,200,250-400,500-650 This field allows a maximum of 200 characters.
Include List (Cont)	If the content of the Include List field has reached the maximum limit of 200 characters, you can continue adding event IDs in this field. This field allows a maximum of 200 characters.
Exclude List	The event IDs that you would like to exclude from the monitoring process using the comma separated value (CSV) format, without any spaces. This field allows a maximum of 200 characters.
Exclude List (Cont)	If the content of the Exclude List field has reached the maximum limit of 200 characters, you can continue adding event IDs in this field. This field also allows a maximum of 200 characters.

Service Detail	Description
Event Source Include Filter	The names of the sources that you would like to include in the monitoring process. The name entered in this field must match the name of the source that is displayed in the Event Properties dialog for the event type. You can obtain the name of the source by double-clicking the event type that you would like to monitor. You must use the CSV format, without any spaces. Example: Userenv,Security,W32Time
Event Source Exclude Filter	The names of the sources that you would like to exclude from the monitoring process. The name entered in this field must match the name of the source that is displayed in the Event Properties dialog for the event type. You can obtain the name of the source by, double-clicking the event type that you would like to exclude from the monitoring process. You must use the CSV format, without any spaces. Example: Userenv,Security,W32Time

Chapter 35

Exchange Server

Service Type:	System
Collection Method:	WMI Server
Instances on a Device:	Single
Supported Platforms:	Microsoft® Exchange Server 2000 and 2003
Device Class:	Windows Server
Monitored By:	Network Windows Probe, Workgroup Windows Probe, WSP
Service Version:	N-central 4.0 and greater

Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* published by Microsoft®.

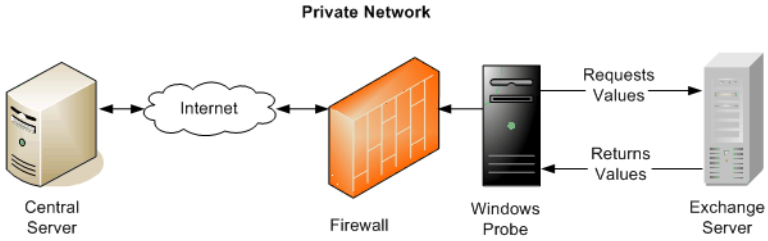
The Exchange Server service uses the Windows probe to monitor the Microsoft Exchange Server for its availability and performance. The results from monitoring are displayed on the status dashboard under the Exchange Server service and, if specified, can also be provided in any notifications triggered by the service.

During the monitoring process, the probe uses the WMI protocol to query the following events on the Exchange Server:

- the number of users currently using the Information Store,
- the public and private Information Store sizes,
- the send queue size of the MS Exchange Information Store Mailbox,
- the receive queue size of the MS Exchange Information Store Mailbox, and
- the Remote Procedure Call (RPC) requests.

Figure 35-1 displays the monitoring process of the Exchange Server service, in which the probe sends the information it receives from the Exchange Server through the firewall to the central server.

Figure 35-1: Monitoring the Exchange Server



To monitor the Exchange Server, you must:

- Add the Exchange Server as a device. For more information, refer to Adding Devices in the *Customer Manual*.
- Add the Exchange Server service to the device. For more information, refer to Adding Services in the *Customer Manual*.

Service Details

Exchange Server Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Public Information Store EDB file	The location of the Exchange Database (EDB) and Streaming Database (STM) files that you would like to monitor. The service monitors the combined size of the files and displays a status based on the specified thresholds on the Windows Services dashboard. These files contain all of the data on the Public Information Store. Access to the Public Information Store is not restricted. The default limit reflects the size of the standard edition, which is 16 GB. These limits should be modified to reflect the actual disk limitations for non-standard versions of the Information Store server. Ensure that you include the double backslashes when specifying your own EDB and STM files.
Public Information Store STM file	
Private Information Store EDB file	The Exchange Database (EDB) and Streaming Database (STM) files that you would like to monitor. The service monitors the combined size of the files and displays a status based on the specified thresholds on the Windows Services dashboard. These files contain all of the data on the Private Information Store. Access to the Private Information Store is restricted. The default limit reflects the size of the standard edition, which is 16 GB. These limits should be modified to reflect the actual disk limitations for non-standard versions of the Information Store server. Ensure that you include the double backslashes when specifying your own EDB and STM files.
Private Information Store STM file	

Status Details

Exchange Server Status Details

Status Detail	Description
The number of people currently using the Information Store	The number of active users who are currently using the Information Store to send and receive messages.
The number of client requests currently being processed by the store	The number of requests that the Information Store is currently handling.
The queue of messages outbound from the Information Store	The number of messages that are in the outbound queue of the Information Store.
The queue of messages inbound to the Information Store	The number of messages that are inbound to the Information Store.
Public Information store size	The size of the Public Information database.
Private Information store size	The size of the Private Information database.

Chapter 36

Fan Status

Fan Status (Dell)

Service Type: System

Collection Method: SNMP

Instances on a Device: Multiple

Supported Platforms: Dell PowerEdge series servers running Dell OpenManage Server Administrator software

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Hardware Probe, Windows Probe

Service Version: N-central 5.0 and greater

The Fan (Dell) service monitors the status and reading (RPMs) of the fans for Dell servers.

Service Details

Fan (Dell) Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	
Cooling Device Location Name Index	The index of the cooling device location name.
Cooling Device Location Name Value	The value of the cooling device location name.

Configuring Cooling Device Location Name Index or Value

To configure this service, you will have to walk the OID .1.3.6.1.4.1.674.10892.1.700.12.1.8 and look at coolingDeviceLocationName.

Example:

```
# snmpwalk -Cp -On -c public -v1 10.20.30.29
.1.3.6.1.4.1.674.10892.1.700.12.1.8


.1.3.6.1.4.1.674.10892.1.700.12.1.8.1.1 = STRING: "ESM MB
Fan1 RPM"
.1.3.6.1.4.1.674.10892.1.700.12.1.8.1.2 = STRING: "ESM MB
Fan2 RPM"
.1.3.6.1.4.1.674.10892.1.700.12.1.8.1.3 = STRING: "ESM MB
Fan3 RPM"
.1.3.6.1.4.1.674.10892.1.700.12.1.8.1.4 = STRING: "ESM MB
Fan4 RPM"
.1.3.6.1.4.1.674.10892.1.700.12.1.8.1.5 = STRING: "ESM MB
Fan7 RPM"
Variables found: 5
```

In this case, there are 5 fans available to monitor. Monitor each fan by adding a task for each entry in the output. Configure the Cooling Device Location Name Index to contain `"1.1"`, `"1.2"`, `"1.3"`, `"1.4"` , or `"1.5"`. Alternatively, configure the Cooling Device Location Name Value to contain `"ESM MB Fan1 RPM"`, `"ESM MB Fan2 RPM"`, `"ESM MB Fan3 RPM"`, `"ESM MB Fan4 RPM"`, or `"ESM MB Fan7 RPM"`.

Status Details

Fan (Dell) Status Details

Status Detail	Description
Fan (Dell) Status	The status of the cooling device.
Fan (Dell) Reading	The speed in revolutions per minute (RPM) of the OFF/ON value of the cooling device.

Fan Status (HP)

Service Type: Network

Collection Method: SNMP

Instances on a Device: Single

Supported Platforms: Compaq/HP ProLiant Series Servers running Compaq Insight Manager v7

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Hardware Probe, Windows Probe

Service Version: N-central 5.0 and greater

The Fan (HP) service monitors the condition of the system and CPU fans for Compaq/HP ProLiant servers.

Service Details

Fan (HP) Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	

Status Details

Fan (HP) Status Details

Status Detail	Description
System Fan Status (Compaq)	The status of the fan(s) in the system. This value will be one of the following: • Other(1) -- Fan status detection is not supported by this system or driver. This maps to Normal in N-central. • Ok(2) -- All fans are operating properly. This maps to Normal in N-central. • Degraded(3) -- A non-required fan is not operating properly. • Failed(4) -- A required fan is not operating properly.
CPU Fan Status (Compaq)	The status of the processor fan(s) in the system. This value will be one of the following: • Other(1) -- Fan status detection is not supported by this system or driver. This maps to Normal in N-central. • Ok(2) -- All fans are operating properly. This maps to Normal in N-central • Failed(4) -- A fan is not operating properly. This maps to Failed in N-central.

Chapter 37

File Size

Service Type: System

Collection Method: WMI Workstation

Instances on a Device: Multiple

Supported Platforms: Any Windows workgroup or server that supports WMI

Device Class: Windows Server and Windows Workstation

Monitored By: Windows Probes

Service Version: N-central 5.0 and greater

Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* published by Microsoft®.

The File Size service monitors the file size, in bytes, as collected from the WMI Class 'CIM_DataFile' Property 'FileSize'.

Service Details

File Size Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	
File Name and Path	The directory path and name of the file that you would like monitored by the service. The directory path and file name must be specified within double quotation marks and delimited by the required double-backslashes. Example: "c:\\Program Files\\Internet Explorer\\iexplore.exe"

Status Details

File Size Status Details

Status Detail	Description
File Size (bytes)	The file size of the service, in bytes.

Chapter 38

Firewall

The Firewall (FW) services allow you to monitor the status of your firewall and generate notifications and trend reports on your firewall's activities. N-central monitors the following types of firewalls:

- Check Point® FireWall -1,
- Cisco® PIX®,
- FortiGate™-200,
- NetScreen® 25,
- SonicWALL® 2040, and
- WatchGuard® Firebox® X500.

Before the monitoring process can begin, the firewall must be added as a device in N-central and set up to send events as security log messages to the monitoring probe. The security log messages are sent using the BSD syslog protocol, an industry-standard protocol used to collect log information on devices. The protocol is defined in REF 3164. The exceptions to this are the FW-Chk Point service and Connections (Cisco Pix) service, which use SNMP polling to collect their metrics.

During the monitoring process, the probe parses these messages with its default regular expressions. Each regular expression is mapped to a status. When a match is found, a status based on the specified thresholds is delayed on the Managed Services dashboard.

Both the regular expressions and the status thresholds can be modified. Each firewall type has its own default regular expressions.These services support wide characters.

Connections (Cisco Pix)

Service Type:	Security
Collection Method:	SNMP
Instances on a Device:	Single
Supported Platforms:	Cisco® PIX®
Device Class:	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Monitored By:	Network Hardware Probe, Network Windows Probe, and Workgroup Windows Probe
Service Version:	N-central 5.0 and greater

For information about the monitoring process, refer to Firewall on page 119.

Service Details

Connections (Cisco Pix) Service Details

Service Detail	Description
Monitoring	Refer to .
Time to Stale	
Service Description	
Scan Interval	
Cisco Firewall Connection Stat Description Index	The index corresponding to the following string: number of connections currently in use by the entire firewall, which is determined by performing an SNMP walk on the cfwConnectionStatTable and locating the cfwConnectionStatDescription (.1.3.6.1.4.1.9.9.147.1.2.2.2.1.3).
Cisco Firewall Connection Stat Description Value	The following string: number of connections currently in use by the entire firewall.
Cisco Firewall Connection Stat Index	The index corresponding to the following string: highest number of connections in use at any one time since system startup, which is determined by performing an SNMP walk on the cfwConnectionStatTable and locating cfwConnectionStatDescription (.1.3.6.1.4.1.9.9.147.1.2.2.2.1.3).
Cisco Firewall Connection Stat Description	The following string: highest number of connections in use at any one time since system startup.

Status Details

Connections (Cisco Pix) Status Details

Status Detail	Description
Current Connections	The number of connections currently in use by the entire firewall.
Max Connections	The highest number of connections in use at any one time since system startup.

Configuring Connections (Cisco Pix)

To configure Connections (Cisco Pix)

Walk the cfwConnectionStatTable table and look at cfwConnectionStatDescription.

Example:

```
# snmpwalk -Cp -On -c public -v1 10.150.1.20
.1.3.6.1.4.1.9.9.147.1.2.2.2.1.3
.1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.6 = STRING: "number
of connections currently in use by the entire firewall"
.1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.7 = STRING:
"highest number of connections in use at any one time
since system startup"
Variables found: 2
```

The default strings for the two parameters in the GUI must correspond to these values.

FW-Chk Point

Service Type: Network

Collection Method: SNMP

Instances on a Device: Single

Supported Platforms: Check Point FireWall-1 v5.4

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Network Hardware Probe, Network Windows Probe, and Workgroup Windows Probe

Service Version: N-central 5.0 and greater

For information about the monitoring process, refer to Firewall on page 119.

The FW-Chk Point service collects vendor-supplied metrics from the .1.3.6.1.4.1.2620 Check Point private branch, such as packets accepted, packets rejected, packets dropped, packets logged, last trap event sent, and so on.

Service Details

FW-Chk Point Service Details.

Service Detail	Description
Monitoring	Refer to .
Time to Stale	
Service Description	
Scan Interval	

Status Details

FW-Chk Point Status Details

Status Detail	Description
Module State	The state of the firewall module.
Filter Name	The name of the loaded filter.
Filter Date	A string describing when the filter was installed.
Accepted Packets	The number of accepted packets.
Rejected Packets	The number of rejected packets.
Dropped Packets	The number of dropped packets.
Logged Packets	The number of logged packets.
Major Version Number	The FireWall-1 major version.
Minor Version Number	The FireWall-1 minor version.
Product	The FireWall-1 product string.
Last Trap Sent	A string containing the last SNMP trap sent from the firewall.

FW-Cisco Pix

Service Type: Security

Collection Method: SNMP

Instances on a Device: Single

Supported Platforms: Cisco® PIX®

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Network Hardware Probe, Network Windows Probe, and Workgroup Windows Probe

Service Version: N-central 3.6 and greater

For information about the monitoring process, refer to Firewall on page 119.

Service Details

The default keywords that are displayed in the regular expression fields are obtained from Cisco® Systems®. For information about these keywords, refer to the Cisco PIX documentation.

FW-Cisco Pix Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Scan Interval	
Regular Expression for Severity 1	
Regular Expression for Severity 2	
Regular Expression for Severity 3	
Regular Expression for Severity 4	

Status Details

FW-Cisco Pix Status Details

Status Detail	Description
Severity 1	An event with a severity of emergency was detected.
Severity 2	An event with a severity of alert was detected.
Severity 3	An event with a severity of error was detected.
Severity 4	An event with a severity of warning was detected.
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	This is the first line of the lines that were scanned, not the first line in the file.

FW-Fortigate

Service Type: Security

Collection Method: Syslog

Instances on a Device: Single

Supported Platforms: Fortinet FortiGate™-200 firmware version 2.80, Linux only

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Network Hardware Probe, Network Windows Probe, and Workgroup Windows Probe

Service Version: N-central 4.5 and greater

For information about the monitoring process, refer to Firewall on page 119.

Service Details

The default keywords that are displayed in the regular expression fields are obtained from Fortigate.

FW-Fortigate Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Scan Interval	
Regular Expression for Emergency	
Regular Expression for Alert	
Regular Expression for Critical	
Regular Expression for Error	
Regular Expression for Warning	

Status Details

FW-Fortigate Status Details

Status Detail	Description
Emergency	The threshold values that determine the status change of the service. If the related regular expression is found, the test is successful. Otherwise, the test is unsuccessful. Based on the test results, the appropriate status is then displayed for the service.
Alert	
Critical	
Error	
Warning	
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	This is the first line of the lines that were scanned, not the first line in the file.

FW-Netscreen

Service Type: Security

Collection Method: Syslog

Instances on a Device: Single

Supported Platforms: NetScreen® 25

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Network Hardware Probe, Network Windows Probe, and Workgroup Windows Probe

Service Version: N-central 3.6 and greater

For information about the monitoring process, refer to Firewall on page 119.

Service Details

The default keywords that are displayed in the regular expression fields are obtained from NetScreen.

FW-Netscreen Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Scan Interval	
Regular Expression for Emergency	
Regular Expression for Alert	
Regular Expression for Critical	
Regular Expression for Error	
Regular Expression for Warning	

Status Details

FW-Netscreen Status Details

Status Detail	Description
Emergency	The threshold values that determine the status change of the service. If the related regular expression is found, the test is successful. Otherwise, the test is unsuccessful. Based on the test results, the appropriate status is then displayed for the service.
Alert	
Critical	
Error	
Warning	
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	This is the first line of the lines that were scanned, not the first line in the file.

FW-SonicWALL

Service Type: Security

Collection Method: Syslog

Instances on a Device: Single

Supported Platforms: SonicWALL® 2040

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Network Hardware Probe, Network Windows Probe, and Workgroup Windows Probe

Service Version: N-central 3.6 and greater

For information about the monitoring process, refer to Firewall on page 119.

Service Details

The default keywords that are displayed in the regular expression fields are obtained from SonicWall.

FW-SonicWall. Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Scan Interval	
Regular Expression for Severity 0	
Regular Expression for Severity 1	
Regular Expression for Severity 2	
Regular Expression for Severity 3	

Status Detail

FW-SonicWall Status Details

Status Detail	Default Keyword
Severity 0	An event with a severity of emergency was detected.
Severity 1	An event with a severity of alert was detected.
Severity 2	An event with a severity of error was detected.
Severity 3	An event with a severity of warning was detected.
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	This is the first line of the lines that were scanned, not the first line in the file.

FW-Watchguard

Service Type: Security

Collection Method: Syslog

Instances on a Device: Single

Supported Platforms: WatchGuard® Firebox® X500

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Network Hardware Probe, Network Windows Probe, and Workgroup Windows Probe

Service Version: N-central 3.6 and greater

For information about the monitoring process, refer to Firewall on page 119.

During the monitoring process, the Firebox 500, which is added as a device in N-central, sends log information to the Network Hardware probe. The probe scans the information using the specified regular expression keywords.

For information about the monitoring process, refer to Firewall on page 119.

Service Details

The default keywords that are displayed in the regular expression fields are used to scan the log information of the Firebox X500. For information about these keywords, refer to the Firebox X500 documentation.

FW-Watchguard Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Scan Interval	
Regular Expression for Fail	
Regular Expression for Warning	

Status Details

FW-Watchguard Status Details

Status Detail	Description
Fail	The threshold values that determine the status change of the service.
Warning	If the related regular expression is found, the test is successful. Otherwise, the test is unsuccessful. Based on the test results, the appropriate status is then displayed for the service.
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	This is the first line of the lines that were scanned, not the first line in the file.

Chapter 39

Frame Relay

Service Type:	Network
Collection Method:	SNMP
Instances on a Device:	Multiple
Supported Platforms:	N/A
Device Class:	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe
Service Version:	N-central 3.5 and greater

Frame Relay is an efficient data transmission technique used to send digital information such as voice, data, local area network (LAN), and wide area network (WAN) traffic quickly and cost-efficiently to many destinations using virtual circuits. Frame Relay is characterized by connection-oriented, permanent or switched virtual circuits (PVC and SVC) at speeds up to 50 Mbps.

When you add the Frame Relay service to a device, N-central scans the device for the interface ifType 32, which is the Frame Relay interface. After N-central locates the Frame Relay interface, you can edit the details of this service.

N-central can monitor the Frame Relay circuit status, congestion notifications and the amount of traffic on the Frame Relay virtual circuits. In addition, thresholds can be set against counters that indicate congestion on the network.

To monitor the Frame Relay service on a device, you must:

- Select the SNMP Enabled option when adding the device. For more information, refer to Adding Devices in the *Customer Manual*.
- Run interface discovery on the device. For more information, refer to Discovering Interfaces for SNMP Services in the *Customer Manual*.
- Add the Frame Relay service to the device. For more information, refer to Adding Services in the *Customer Manual*.
- After interface discovery is complete, set the Which Interface to scan service detail for the Frame Relay service. For more information, refer to Setting Interfaces for SNMP Services in the *Customer Manual*.

The tables IF-MIB and FRAME-RELAY-DTE-MIB describe the SNMP objects that are queried by the probe.

IF-MIB

Object Descriptors	Numerical OID
sysUptime	1.3.6.1.2.1.1.3
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
ifSpeed	1.3.6.1.2.1.2.2.1.5

FRAME-RELAY-DTE-MIB

Object Descriptors	Numerical OID
frCircuitIfIndex	1.3.6.1.2.1.10.32.2.1.1
frCircuitState	1.3.6.1.2.1.10.32.2.1.3
frCircuitReceivedFECNs	1.3.6.1.2.1.10.32.2.1.4
frCircuitReceivedBECNs	1.3.6.1.2.1.10.32.2.1.5
frCircuitSentFrames	1.3.6.1.2.1.10.32.2.1.6
frCircuitSentOctets	1.3.6.1.2.1.10.32.2.1.7
frCircuitReceivedFrames	1.3.6.1.2.1.10.32.2.1.8
frCircuitReceivedOctets	1.3.6.1.2.1.10.32.2.1.9

Service Details

Frame Relay Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Service Description	
Scan Interval	
Interfaces to Monitor	The name of the interface that is being monitored.

Status Details

Frame Relay Thresholds Status Details

Status Detail	Description
Thresholds	N-central applies thresholds metrics based on the virtual circuit. N-central determines the monitored data against the specified threshold values.
Octets (Transmitted and Received)	The total number of transmitted and received octets.
Frames (Transmitted and Received)	The total number of transmitted and received frames.

Status Detail	Description
Average Packet Size	The average number of octets sent and received over this virtual circuit calculated as a percentage of the total capacity of the virtual circuit: Average frame size= total transmitted and received octets divided by total transmitted and received frames This threshold is measured in octets.
Transmit Utilization (percentage)	The number of octets transmitted over the Frame Relay virtual circuit during a scan interval time, which is calculated as a percentage of the total capacity of the virtual circuit: Transmitted utilization during a scan interval: Transmitted Octets divided by (Virtual Circuit Speed multiplied by Scan Interval) Transmitted octets is the difference between the number of octets transmitted during the previous scan and the number of octets transmitted during the current scan. This threshold is measured as a percentage value.
Receive Utilization	The number of octets received over the Frame Relay virtual circuit during a scan interval time, which is calculated as a percentage of the total capacity of the virtual circuit: Received Utilization during a scan interval= Received Octets divided by (Virtual Circuit Speed multiplied by Scan Interval) Received octets is the difference between the number of octets received during the previous scan and the number of octets received during the current scan. This threshold is measured as a percentage value.
Forward Explicit Congestion Notification	This type of notification is transmitted from the source terminal requesting the destination terminal to slow its requests for data. The notification occurs when the data capacity level of the source terminal reaches the value set by the data terminal equipment (DTE), or when a switch queues a frame to a trunk that is congested. This field displays the number of FECNs received from the network indicating forward congestion since the virtual circuit was created. The FECN is calculated as: current received FECNs minus old received FECNs This threshold is measured in frames.
Backward Explicit Congestion Notification	This type of notification is transmitted from the destination terminal requesting the source terminal to slow its data transmission. The notification occurs when the data capacity level of the destination terminal reaches the value set by the data terminal equipment (DTE), or when a switch receives a frame from a trunk that is congested. This field displays the number of BECNs received from the network indicating forward congestion since the virtual circuit was created. The BECN is calculated as: current received BECNs minus old received BECNs This threshold is measured in frames.
Circuit Status	Indicates whether the particular virtual circuit is operational.

Chapter 40
FTP

Service Type: Network

Collection Method: TCP

Instances on a Device: Single

Supported Platforms: N/A

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server

Service Version: N-central 3.0 and greater

The FTP service supports file transfers between local and remote computers.

The File Transfer Protocol (FTP) test checks the status of the FTP service on the network device. During the test, N-central can determine the availability status of the FTP service by comparing the availability of the FTP service to the threshold value.

Service Details

FTP Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Timeout Value	
Port Number	
Validating String	

Status Details

FTP Status Details

Status Detail	Description
FTP Service Availability	N-central determines whether the FTP service is up or down. The FTP service does not use thresholds or the Warning state.
Round Trip Time (ms)	The time (in milliseconds) for a request to be sent and received.
DNS Resolution	The threshold that determines whether the device name can be resolved. If an FQDN has been specified, the service searches for its IP address. If the IP address is found, the state will be Normal. Otherwise, it will be Failed, based on the default settings. If an IP address has been specified, the service checks only the IP address's format. If the format is correct, the state will be Normal. Otherwise, it will be Failed, based on the default settings.

Chapter 41

Generic ODBC

Service Type: Network

Collection Method: ODBC

Instances on a Device: Multiple

Supported Platforms: Microsoft® SQL Server

Device Class: Generic Server and Windows Server

Monitored By: Agent (Windows, RedHat, and Suse), Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP

Service Version: N-central 5.0 and greater

The Generic ODBC service monitors the results of any query sent to an MS SQL or Postgres SQL database using Open Database Connectivity (ODBC), which is a standard application program interface (API). The results are obtained through regular expression matching and displayed on the status dashboard under the Generic ODBC service. If specified, the results can also be provided in any notifications triggered by the service.

For example, the number of times that "Error" appears in a database table, which tracks the status of a process, can be queried and monitored using regular expression matching. If found, the status of the service can display Failed, according to specified thresholds.

Up to 10 instances of this service can be monitored, therefore, up to 10 queries can be monitored at a time. For this service, the "mixed mode" option for the Microsoft SQL server and the correct ODBC driver information must be specified. For more information about setting up the SQL server in "mixed mode", refer to Setting Up the SQL Server in Mixed Mode on page 137. The table ODBC Driver Support provides the names and versions of the ODBC drivers that support the agents and probes that can be used to monitor this service.

Note: This service is not supported by the Novell agent.

ODBC Driver Support

Agent/Probe	ODBC Driver and Version		
	MDAC ODBC Driver 2.8	Unix ODBC Driver 2.2.10	Postgres SQL ODBC Driver 8.01
Windows Agent	x		
RedHat Agent		x	x
Suse Agent		x	x

Agent/Probe	ODBC Driver and Version		
	MDAC ODBC Driver 2.8	Unix ODBC Driver 2.2.10	Postgres SQL ODBC Driver 8.01
Windows Probe	x		
Network Hardware Probe	Provided with an ODBC driver.		

Service Details

Generic ODBC Service Details

Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	
ODBC Driver Name	The name of the ODBC driver that allows the Generic ODBC service to query the specified database.
Database Port	The port on which the database accepts incoming queries.
Database Name	The name of the database used for the query.
Database Username	The username that is used to access the database.
Database Password	The password that is used to access the database.
Database Query	The SQL query statement that is submitted to the database.
Column 1 Name	The name of the database column that is queried for the value.
Column 2 Name	
Column 3 Name	
Column 1 Regular Expression	The regular expression that matches the value in the column. For more information, refer to Table 1-1 on page 2. Ensure that when using the * symbol in a regular expression that you also include the “.” before. Otherwise, the number of matches returned will be inconsistent.
Column 2 Regular Expression	
Column 3 Regular Expression	

Status Details

Generic ODBC Status Details

Status Detail	Description
Transaction time in milliseconds	The total transaction time (in milliseconds) to connect, authenticate, send a query, retrieve results, and disconnect.
Rows returned by the query	The number of rows returned by a query.
Rows returned by the query that matched all column regular expressions	The number of rows that matched all of the column regular expressions.

Setting Up the SQL Server in Mixed Mode

Before the Generic ODBC service can monitor the results of the discovered jobs that have been performed by the MS SQL database, you must set up the SQL server in “mixed mode”.

To set up the SQL server in mixed mode

1. Click Start>All Programs>Microsoft SQL Server>Enterprise Manager.

   ↳ The SQL Server Enterprise Manager screen appears.

2. In the navigation pane, expand Microsoft SQL Servers and then expand SQL Server Group.
3. Right-click on the SQL server that you would like to set up.
4. Select Properties.

   ↳ The SQL Server Properties dialog appears.

5. Select the Security tab.
6. Under Authentication, select SQL Server and Windows.
7. Click OK.

Chapter 42

Generic SNMP

Generic Integer (SNMP)

Service Type:	Network
Collection Method:	SNMP
Instances on a Device:	Multiple
Supported Platforms:	N/A
Device Class:	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe
Service Version:	N-central 4.0 and greater

The Generic Integer (SNMP) service can be set up to monitor any numeric variable by using the Simple Network Management Protocol (SNMP). This service monitors one integer value at a time by allowing you to specify the SNMP object identifier (OID) and the index of the object that you would like to monitor.

The OID represents a particular device metric that is generated from a particular device function. The OID can be up to any 32-bit integer, which can include numeric Boolean values and percentage values that do not have a “%” sign. You can monitor up to 10 instances of the Generic SNMP service.

You can obtain the index of the object that you would like to monitor by performing an SNMP walk on your device. The SNMP walk displays the entire alias of the gauge, its representing OID, and the instance.

Using the snmpwalk command from the net-snmp project package, some options can be specified to display the entire textual representation of an object identifier and the indices of each object instance.

Command:

```
snmpwalk -Of -c public -v 1 192.168.20.146 .1.3.6.1.2.1.2.2.1.8
```

Result:

```
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOp-
erStatus.1 = INTEGER: up(1)
.iso.org.dod.internet.mgmt.mib-
2.interfaces.ifTable.ifEntry.ifOperStatus.2 = INTEGER: up(1)
```

where:	is:
1.3.6.1.2.1.2.2.1.8	The numeric representation of the OID.
iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.iflnErrors	The textual representation of the OID.
ifTable	The name of the table.
ifEntry	The container for the order of the columns.
ifOperStatus	The name of the column. The subsequent number is the index.
1 or 2	The indices.
INTEGER: up (1)	The data type, translated name, and value for this instance.

Each number in the numerical representation of the OID corresponds to a textual identifier in the textual representation. For example, in ".1.3.6.1": 1 represents "iso", 3 represents "org", 6 represents "dod", 1 represents "internet", and so on.

Service Details

Generic Integer (SNMP) Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Target OID Index	The Index of the OID that you would like to monitor.
Target OID Variable	The OID of the gauge that you would like to monitor.
Start Time	Refer to Table 1-1 on page 2.
End Time	
Scan Interval	
Repeat Weekly on Day(s)	
Repeat Monthly on Day(s)	

Status Details

Generic Integer (SNMP) Status Details

Status Detail	Description
OID Value	Monitors the instance, which is obtained by combining the value of the target OID index and the target OID variable that are set on the Service Details tab.

Generic String (SNMP)

Service Type:	Network
Collection Method:	SNMP
Instances on a Device:	Multiple (up to 1000 instances)
Supported Platforms:	N/A
Device Class:	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe
Service Version:	N-central 5.0 and greater

The Generic String (SNMP) service will collect any OID using a configurable OID parameter field. It is returned as a string in N-central's database regardless of the original SNMP data type. Thresholds cannot be applied to Generic String; this is the difference between Generic String (SNMP) and Generic Integer (SNMP).

The Generic String (SNMP) service can be set up to monitor any variable by using the Simple Network Management Protocol (SNMP). This service monitors one value at a time by allowing you to specify the SNMP object identifier (OID) and the index of the object that you would like to monitor.

The OID represents a particular device metric that is generated from a particular device function.

You can obtain the index of the object that you would like to monitor by performing an SNMP walk on your device. Using the snmpwalk command from the net-snmp project package, some options can be specified to display the entire textual representation of an object identifier and the indices of each object instance.

Command:

```
snmpwalk -Of -c public -v 1 192.168.20.146 .1.3.6.1.2.1.2.2.1.8
```

Result:

```
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOp-
erStatus.1 = INTEGER: up(1)
.iso.org.dod.internet.mgmt.mib-
2.interfaces.ifTable.ifEntry.ifOperStatus.2 = INTEGER: up(1)
```

where:	is:
1.3.6.1.2.1.2.2.1.8	The numeric representation of the OID.
iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.iflnErrors	The textual representation of the OID.
ifTable	The name of the table.
ifEntry	The container for the order of the columns.
iflnErrors	The name of the column. The subsequent number is the index.
16777219	The instance.
Counter32: 0	The type and value at the instance 16777219.

Each number in the numerical representation of the OID corresponds to a textual identifier in the textual representation. For example, in ".1.3.6.1": 1 represents "iso", 3 represents "org", 6 represents "dod", 1 represents "internet", and so on.

Service Details

Generic String (SNMP) Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Target OID Index	The Index of the object that you would like to monitor.
Target OID Variable	The OID that you would like to monitor.
Start Time	Refer to Table 1-1 on page 2.
End Time	
Scan Interval	
ObjectID - .1.3.6.1	The unfinished OID. Append the rest of the dotted decimal values that correspond to the snmp object you wish to query to this unfinished OID. For example, if the OID is .1.3.6.1.2.1.2.2.1.8, enter .2.1.2.2.1.8. You must also include the index. For example, to collect the sysDescr system description, enter 2.1.1.1.0 in this field.

Status Details

Generic String (SNMP) Status Details

Status Detail	Description
Generic String	The returned string.
System Uptime	The uptime of the device. This status detail is required.

Chapter 43

Generic SQL Server

Service Type:	Network
Collection Method:	Generic TCP
Instances on a Device:	Multiple (up to 3 instances)
Supported Platforms:	Microsoft® SQL Server
Device Class:	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server
Service Version:	N-central 4.5 and greater

The Generic SQL Server service monitors the availability of the port on which the MS SQL Server application runs. The availability of the port, which is determined by the service testing the port's connectivity, indicates that the MS SQL Server application is running. This service also measures the domain name system (DNS) resolution and the round trip time of the initial connection request and response. The availability results of the TCP service are then reflected on the status dashboard for the Generic SQL Server service.

A maximum of three instances of this service can be set on a device, with each instance monitoring a different port on the device.

The Generic SQL Server service does not use the Warning state.

Service Details

Generic SQL Server Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Timeout Value	
Port Number	

Status Details

Generic SQL Server Thresholds

Status Detail	Description
Generic SQL Server Availability	The threshold that determines the availability of the port.
Round Trip Time (ms)	The time (in milliseconds) for a request to be sent and received.
DNS Resolution	The threshold that determines whether the device name can be resolved. If an FQDN has been specified, the service searches for its IP address. If the IP address is found, the state will be Normal. Otherwise, it will be Failed, based on the default settings. If an IP address has been specified, the service checks only the IP address's format. If the format is correct, the state will be Normal. Otherwise, it will be Failed, based on the default settings.

Chapter 44

Generic (TCP)

Service Type:	Network
Collection Method:	Generic TCP
Instances on a Device:	Multiple (up to 6 instances)
Supported Platforms:	N/A
Device Class:	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server
Service Version:	N-central 3.0 and greater

The Generic (TCP) service monitors the connectivity of a socket on a specified port on a device and, if the port is available, a specific TCP service functioning on the port.

After the port has successfully passed the test for connectivity, the Generic (TCP) service can continue on to use an appropriate command string to test the TCP service it is monitoring and a validation string against which to check the response it receives. The availability results of the TCP service are then reflected on the status dashboard for the Generic (TCP) service. For example, the command string 201 receiving the appropriate response code 220 indicates that the FTP service is running and available for use. The service also measures the round trip time for the request and the domain name system (DNS) resolution.

A maximum of six instances of the Generic (TCP) service can be set on a device, with each instance monitoring a different port on the device.

The Generic (TCP) service does not use the Warning state.

Service Details

Generic (TCP) Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Timeout Value	
Port Number	
Send Command String	A predefined set of characters specific to the TCP service. The string is transmitted upon connection to the host and requests the response about the TCP service.
Validating String	A regular expression that determines whether the response sent by the queried device is valid. For more information, refer to Table 1-1 on page 2.

Status Details

Generic (TCP) Status Details

Status Detail	Description
Generic Service Availability	The threshold that determines the availability of the port.
Round Trip Time (ms)	The time (in milliseconds) for a request to be sent and received.
DNS Resolution	The threshold that determines whether the device name can be resolved. If an FQDN has been specified, the service searches for its IP address. If the IP address is found, the state will be Normal. Otherwise, it will be Failed, based on the default settings. If an IP address has been specified, the service checks only the IP address's format. If the format is correct, the state will be Normal. Otherwise, it will be Failed, based on the default settings.

Chapter 45
HTTP

Service Type: Network

Collection Method: TCP

Instances on a Device: Multiple

Supported Platforms: N/A

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server

Service Version: N-central 3.0 and greater

The Hyper Text Transfer Protocol (HTTP) service monitors a Web server to ensure it is running and publishing Web pages, without reporting any errors. The HTTP service must be added on the Web server, which must also be added as a device in N-central.

During the monitoring process, the HTTP service first attempts to resolve the domain name system (DNS) entry for the Web server. If the DNS test is successful, the service then checks the availability and response time of the Web server using a specified URL. If the DNS test is not successful, the service changes to the Misconfigured state. A code in the response header from the Web server determines whether the server is in a Normal, Warning, or Failed state. The Normal or Warning response codes are tracked as parameters on the status dashboard. The Failed response codes are automatically change the service to the Failed state.

Service Details

HTTP Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Timeout Value	
Port Number	
Validating String	

Service Detail	Description
HTTP URL	The URL used to test the availability of the Web server. For example: • www.xyz.com, • index.html, • http://www.xyz.com/index.html, or • http://www.xyz.com/ A partial URL of the network routable address of the Web server can also be used.
Normal Response Code	The codes in the response header that indicate a Normal state.
Warning Response Code	The codes in the response header that indicate a Warning state.

Status Details

HTTP Status Details

Status Detail	Description
HTTP Service Availability	The availability of a Web server.
Round Trip Time (ms)	The time (in milliseconds) for a request to be sent and received.
DNS Resolution	The FQDN or IP address that determines whether the device name can be resolved. If an FQDN has been specified, the service searches for its IP address. If the IP address is found, the state will be Normal. Otherwise, it will be Failed, based on the default settings. If an IP address has been specified, the service checks only the IP address' format. If the format is correct, the state will be Normal. Otherwise, it will be Failed, based on the default settings.

•

Chapter 46
HTTPS

Service Type: Network

Collection Method: TCP

Instances on a Device: Multiple

Supported Platforms: N/A

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server

Service Version: N-central 4.5 and greater

The Hypertext Transfer Protocol over Secure Socket Layer (HTTP over SSL or HTTPS) service monitors all of the scan details of the HTTP service and the validity and expiry date of an SSL certificate on a device. The scan details for the SSL certificates can be monitored only if the certificates have been signed by a Certificate Authority (CA) that has been uploaded in the N-central Administrator Console (NAC) or is listed in the default CA certificate file provided by N-central. For information about uploading the CA Certificate of an SSL certificate, contact your administrator. For more information about the HTTP scan details that also pertain to this service, refer to HTTP on page 147.

Service Details

HTTPS Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Timeout Value	
Port Number	

Service Detail	Description
HTTPS URL	The URL used to test the availability of the Web server. For example: • www.xyz.com, index.html, • http://www.xyz.com/index.html, or • http://www.xyz.com/ A partial URL is accessed using the network routable address of the Web server.
Normal Response Code	The codes in the response header that indicate a Normal state.
Warning Response Code	The codes in the response header that indicate a Warning state.

Status Details

HTTPS Status Details

Status Detail	Description
HTTPS Service Availability	The availability of a Web server. If the CA certificate of the Web server has not been uploaded nor in the default CA certificate file, this threshold will display Failed.
Round Trip Time (ms)	The time (in milliseconds) for a request to be sent and received.
DNS Resolution	The FQDN and IP address that determines whether the device name can be resolved. If an FQDN has been specified, the service searches for its IP address. If the IP address is found, the state will be Normal. Otherwise, it will be Failed, based on the default settings. If an IP address has been specified, the service checks only the IP address' format. If the format is correct, the state will be Normal. Otherwise, it will be Failed, based on the default settings.
Server Certificate Signature	The number of days remaining before the expiration of the SSL certificate.
Server Certificate Expiration (days)	The regular expression that triggers the status for the matched contents on the Web page.

Chapter 47
IIS

Service Type: System

Collection Method: WMI Workstation

Instances on a Device: Single

Supported Platforms: Microsoft® IIS

Device Class: Windows Server and Windows Workstation

Monitored By: Network Windows Probe, Workgroup Windows Probe, WSP

Service Version: N-central 4.0 and greater

Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* published by Microsoft®.

The IIS service monitors the availability and performance of the Microsoft® Internet Information Server (IIS), which is a group of server applications that are compatible with the Windows NT and Windows 2000 Server operating systems. The IIS sets up and administers Web sites and search engines, and supports the writing of Web-based applications that access databases.

During the monitoring process, the IIS service uses the Windows probe to measure the IIS server's key metrics. The results are displayed on the Windows Services dashboard.

Service Details

IIS Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Web Site Instance Name	The name of the Web site that you would like to monitor.

Status Details

IIS Status Details

Status Detail	Description
Send and receive bytes/sec	The total number of bytes that the server sent and received per second.
Connection attempts/sec	The total number of attempts made to connect to the Web per second.
Total anonymous users/sec	The total number of anonymous users who accessed a Web page per second.
Total known users/sec	The total number of known users who accessed a Web page, per second.
Total current connections	The total number of current Web connections.
Total “Get” requests/sec	The total number of "Get" requests made to retrieve Web sites per second.
Total log-on attempts/sec	The total number of attempts made to log-on to a Web service per second.

Chapter 48

IMAP

Service Type:	Network
Collection Method:	TCP
Instances on a Device:	Single
Supported Platforms:	N/A
Device Class:	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server
Service Version:	N-central 3.0 and greater

The Internet Message Access Protocol (IMAP) test checks the status of the IMAP process on the network device. IMAP is an email protocol that allows a client to access email messages on a server.

N-central can determine the up or down status of the IMAP service. The IMAP service does not use the Warning state.

N-central averages the availability of the IMAP service over the scan interval. It compares the availability of the IMAP service to the threshold to determine the status.

Service Details

IMAP Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan interval	
Timeout Value	
Port Number	
Validating String	

Status Details

IMAP status Details

Status Detail	Description
IMAP Service Availability	N-central determines whether the IMAP service is up or down. The IMAP service does not use the Warning state. N-central averages the availability of the IMAP service over the scan interval and compares the availability of the IMAP service to the threshold to determine the status.
Round Trip Time (ms)	The time (in milliseconds) for a request to be sent and received.
DNS Resolution	The threshold that determines whether the device name can be resolved. If an FQDN has been specified, the service searches for its IP address. If the IP address is found, the state will be Normal. Otherwise, it will be Failed, based on the default settings. If an IP address has been specified, the service checks only the IP address's format. If the format is correct, the state will be Normal. Otherwise, it will be Failed, based on the default settings.

Chapter 49

Intel® vPro™ Status

Service Type: Network

Collection Method: TCP

Instances on a Device: Multiple

Supported Platforms: Intel® vPro™

Device Class: Windows Server

Monitored By: Network - Windows probe, Workgroup - Windows probe

Note: The Workgroup - Windows probe is not available in N-central OnDemand.

Service Version: N-central 6.0 and greater

The Intel® vPro™ Status service monitors the network availability of the Intel® vPro™ interface and the power status of an Intel® vPro™ device.

Service Details

Service Detail	Description
Monitoring	The status of the Intel® vPro™ Status service: • Enabled, which begins the immediate monitoring of the service on the device. • Disabled, which prevents monitoring of the service on the device. To temporarily stop the monitoring process, disable the service. Do not delete the service.
Time to Stale	The time (in minutes) for the most recent monitored data to become stale. The value must be greater than or equal to the scan interval value. Otherwise, the service will be constantly in the Stale state.
Current Monitoring Probe	The central server, probe, or local agent that is to be used to monitor the service.
Service Description	A description of the service.
Scan Interval	The time (in minutes) between each scan.

Service Detail	Description
Port Number	The TCP port number used to monitor a specific Intel® vPro™ device.
Normal Response Code	A response code is returned when an Intel® vPro™ device is queried. A response code of 0 or 11 indicates a normal status.

Status Details

Status Detail	Description
Network Connectivity	The availability of the Intel® vPro™ interface: • Normal = The interface is available. • Failed = The interface is unavailable.
Power Status	The power status of the Intel® vPro™ device: • Normal = The device is on. • Failed = The device is off.

Chapter 50

Intrusion Detection

Service Type:	Security
Collection Method:	Log Appended
Instances on a Device:	Single
Supported Platforms:	Snort™ and IDS applications
Device Class:	Generic Server, Generic Workstation, Windows Server, and Windows Workstation
Monitored By:	Agent (Windows, Novell Netware, RedHat Linux, RedHat Enterprise Linux, and Suse Linux)
Service Version:	N-central 3.0 SP3 and greater

The Intrusion Detection service monitors events that are generated by Snort™ and any other intrusion detection applications installed on your network.

The intrusion detection application searches the network packets for suspicious patterns that match its predefined class-types and logs them to a local log file or to its database. If the intrusion detection application has been configured to log its events to a local log file, then N-central can monitor the application.

During the monitoring process, the agent that is used for the Intrusion Detection service scans the log file for any keywords that match the regular expressions specified for the service. If a match is found, the agent reports it to the central server. Based on the specified threshold, N-central then displays the appropriate status for the service.

If the status triggers a notification, the notification includes the first line and the line numbers on which the keyword was found unless a numeric pager was used for the notification. The first line and any subsequent line numbers are also displayed in the applicable reports and on the status details screen for the service. This service also supports wide characters.

By default, the Snort class-types are contained in the service's regular expressions, which are classified as Failed or Warning.

Note: The Intrusion Detection service is supported by the Linux agent and all of the Windows agents, but not by the Novell agents and Network hardware probes.

Service Details

Intrusion Detection Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Scan Interval	
Regular Expression 1	
Regular Expression 2	
Regular Expression 3	
Regular Expression 4	
Log File Name and Path	

Status Details and Class Types

Intrusion Detection Status Details and Associated Class Types

Status Details	Class Type	Description
Critical (1) Regular Expression 1	attempted-admin	Attempted Administrator Privilege Gain
	attempted-user	Attempted User Privilege Gain
	shellcode-detect	Executable code was detected
	successful-user	Successful Administrator Privilege Gain
	successful-admin	Successful User Privilege Gain
Critical (2) Regular Expression 2	trojan activity	A Network Trojan was detected
	unsuccessful-user	Unsuccessful User Privilege Gain
	web-application attack	Web Application Attack
Warning (1) Regular Expression 3	attempted-dos	Attempted Denial of Service
	attempted-recon	Attempted Information Leak
	bad-unknown	Potentially Bad Traffic
	denial-of-service	Detection of a Denial of Service Attack
	misc-attack	Misc Attack
	non-standard-protocol	Detection of a non-standard protocol or event
	rpc-portmap-decode	Decode of an RPC Query
	successful-dos	Denial of Service
	successful-recon-largescale	Large Scale Information Leak
	successful-recon-limited	Information Leak
	suspicious-filename-detect	A suspicious filename was detected
	suspicious-login	An attempted login using a suspicious username was detected

Status Details	Class Type	Description
Warning (2) Regular Expression 4	system-call-detect	A system call was detected
	unusual-client-port-connection	A client was using an unusual port
	web-application-activity	access to a potentially vulnerable web application
The line count matched regex...	Off	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched		The first 250 characters of the first line, in the log file, containing the matching keyword returned by the agent. This information is displayed on the service's status details screen, any applicable reports, and any triggered notifications (except for numeric pages).

Chapter 51
ISA

Service Type:	System
Collection Method:	WMI Workstation
Instances on a Device:	Single
Supported Platforms:	Microsoft® ISA server and the enterprise edition of the ISA server 2000
Device Class:	Windows Server and Windows Workstation
Monitored By:	Network Windows Probe, Workgroup Windows Probe, WSP
Service Version:	N-central 4.0 and greater

Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* published by Microsoft®.

The ISA service monitors the availability of the Microsoft® Internet Security and Acceleration (ISA) server, which serves as an enterprise firewall and a cache server. The ISA firewall scans circuit, application, and packet data and the ISA cache server manages Web page requests and provides faster access to frequently used sites by saving them.

During the monitoring process, the ISA service uses the Windows probe to measure the ISA server's key metrics. The results are then displayed on the dashboard for the service.

Service Details

ISA Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	

ISA Status Details

Status Detail	Description
Inbound bandwidth	The amount of incoming traffic.
Outbound bandwidth	The amount of outgoing traffic.
Current active sessions	The total number of current Web sessions.
Packets dropped by filter denial	The total number of packets that were dropped based on the firewall policies set by your organization.
Packets dropped by protocol breach	
Cache running hit ratio (%)	The hit rate for the last specified number of requests. This helps you determine the current performance of the ISA server's cache.
Total requests/sec	The number of times data is requested from a cache per second.

Chapter 52

License Compliance

Service Type:	System
Collection Method:	System
Instances on a Device:	Single (one for each customer account)
Supported Platforms:	Microsoft® Windows®
Device Class:	Windows Server and Windows Workstation
Monitored By:	Network Windows Probe, Workgroup Windows Probe, WSP
Service Version:	N-central 4.5 and greater

Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* published by Microsoft®.

The License Compliance service monitors the limit of application licenses allowed for a customer. For example, if a customer is allowed 100 licenses for one application and uses 88, then a Warning state for this service can notify the customer that 88% of the available licenses are in use.

This service is available only for Windows devices on which assets have been discovered. By default, its state can be viewed on the Asset Services dashboard. For information about setting this service's details and thresholds, refer to Setting the License Compliance Service Details in the *Customer Manual*.

Chapter 53

Local IP

Service Type: System

Collection Method: Local API

Instances on a Device: Single

Supported Platforms: N/A

Device Class: Generic Server, Generic Workstation, Windows Server, and Windows Workstation

Monitored By: Agent (Windows)

Service Version: N-central 3.0 and greater

The Local IP test allows you to keep the N-central database up to date by checking the IP address of a monitored device. The Local IP test returns the IP address of the monitored device to the central server and displays it on the details screen for a device. You should use the Local IP test to monitor networks that use dynamic IP addressing.

If you would like to monitor the local IP of a device, you select Update Monitored Address on the Agent tab of the device. Selecting this option causes the central server to update the device's network routable address that is monitored by the server or Network Hardware probe. The central server updates the address when the device's local IP address changes based on the information gathered by the agent on the device.

N-central does not monitor the status of the Local IP service and cannot create reports for it.

Service Details

Local IP Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Scan Interval	

Chapter 54

Log Analysis (Appended)

Service Type: System

Collection Method: Log Appended

Instances on a Device: Multiple

Supported Platforms: N/A

Device Class: Generic Server and Windows Server

Monitored By: Agent (Windows and Mac OSX 10.4)

Service Version: N-central 3.0 and greater

The Log Analysis (Appended) is an agent-based service and works only on log files that are located on a file system that is local to the agent. It allows you to monitor text that an application, such as a Web server or a firewall, writes to its log file. During the monitoring process, the service executes a check on the log file at regular intervals, and it scans logged lines that were added to the file since its last execution. Through the use of regular expression matching and timestamp comparison, this service can notify you when the application stops logging to its log file, or when it logs an error or a warning message. This service monitors up to 4 log files for each device and supports wide characters.

Service Details

Log Analysis (Appended) Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Scan Interval	
Log File Name and Path	
Regular Expressions (1 to 6)	

Status Details

Log Analysis (Appended) Status Details

Status Detail	Description
File Size (Bytes)	N-central reads the size of the file and compares it with the values your threshold specifications. Threshold options can vary for each specified regular expression.
Regular Expressions (1 to 6)	The thresholds for the regular expressions that you specified on the Service Details tab.
Difference in minutes...	N-central compares the values that you specify in this field with the age of the log file that is calculated by the agent. The age is the difference between the time the log file was generated and the current time.
Line Count of Log File	The number of lines in the file that are scanned and compared with your threshold specifications.
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	The first 250 characters of the first line, in the log file, containing the matching keyword returned by the agent. This information is displayed on the service's status details screen, any applicable reports, and any triggered notifications (except for numeric pages).

Chapter 55

Log Analysis (Batch)

Service Type:	System
Collection Method:	Log Batch
Instances on a Device:	Multiple
Supported Platforms:	N/A
Device Class:	Generic Server and Windows Server
Monitored By:	AAgent (Windows, Novell Netware, RedHat Linux, RedHat Enterprise Linux, Suse Linux, and Mac OSX 10.4)
Service Version:	N-central 3.0 and greater

The Log Analysis (Batch) is an agent-based service and works only on log files that are located on a file system that is local to the agent. It allows you to monitor text that N-central writes to a log file during the execution of a scheduled process or task, such as a nightly virus scan or a weekly backup. During the monitoring process, the service scans the complete log file created during the scheduled process. Through the use of regular expression matching and timestamp comparison, it ensures that the task was completed successfully.

Each time N-central or the application performs a scheduled task or process, it creates a new Batch log file. The names of the files are numbered in sequence according to a specific application's recording convention. The Log Analysis (Batch) service uses the latest modified date as the metric to determine which log file it should scan during the monitoring process. This service monitors up to 4 log files for each device and supports wide characters.

Service Details

Log Analysis (Batch) Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Log File Name and Path	
Start Time	
End Time	
Scan Interval (minutes)	
Repeat Weekly on Day(s)	
Repeat Monthly on Day(s)	
Regular Expressions (1 to 6)	

Status Details

Log Analysis (Batch) Status Details

Status Detail	Description
File Size (Bytes)	N-central reads the size of the file and compares it with the values your threshold specifications. Threshold options can vary for each specified regular expression.
Regular Expressions (1 to 6)	The thresholds for the regular expressions that you specified on the Service Details tab.
Last Parse-able Dates Time Zone	The time zone off-set based on Greenwich Mean Time (GMT) or Universal Time Coordinated (UTC).
Difference in minutes...	N-central compares the values that you specify in this field with the age of the log file that is calculated by the agent. The age is the difference between the time the log file was generated and the current time.
Number of lines in the file	N-central scans the number of lines in the file and compares it with your threshold specifications.
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	The first 250 characters of the first line, in the log file, containing the matching keyword returned by the agent. This information is displayed on the service's status details screen, any applicable reports, and any triggered notifications (except for numeric pages).

Chapter 56

Logical Drive and RAID

Logical Drive (Dell)

The Logical Drive service monitors the overall status of logical drives represented by this service for Dell.

Service Details

Logical Drive Status (Dell) Service Details

Service Detail	Description
Monitoring	Refer to .
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	
virtualDiskState Index	The index of the virtual Disk State object. The OIDs are: .1.3.6.1.4.1.674.10893.1.1.140.1.1.4 virtualDiskState .1.3.6.1.4.1.674.10893.1.1.140.1.1.5 virtualDiskSeverity.

Scan Details

Logical Drive (Dell)

Status Detail	Description
Logical Drive (Dell) Status	The status of the logical drive.
Logical Drive (Dell) Severity	The severity of the logical drive.

RAID Status (HP)

Service Type: Network

Collection Method: SNMP

Instances on a Device: Single

Supported Platforms: Compaq/HP ProLiant Series Servers running Compaq Insight Manager v7

Device Class: Generic Server and Windows Server

Monitored By: Hardware Probe and Windows Probes

Service Version: N-central 5.0 and greater

The RAID Status (HP) service monitors the overall status of the disk array represented by this service for Compaq/HP ProLiant servers.

Service Details

RAID Status (HP) Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	

Status Details

RAID Status (HP) Status Details

Status Detail	Description
RAID Status (HP)	The overall condition status of the disk array.

Chapter 57

MBSA 1.2.1

Service Type:	Security
Collection Method:	WMI Workstation and MBSA
Instances on a Device:	Single
Supported Platforms:	Microsoft® Windows®
Device Class:	Windows Server and Windows Workstation
Monitored By:	Network Windows Probe, Workgroup Windows Probe **Note:** Network Windows probes are not available as part of N-central OnDemand.
Service Version:	N-central 4.0 and greater

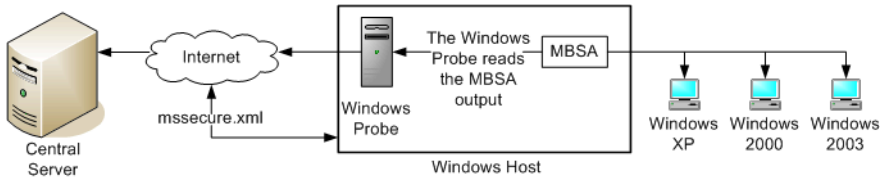
Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* published by Microsoft®.

The MBSA 1.2.1 service supports MBSA version 1.2.1 and has the option to support SUS version 1.0. It ensures that your Windows devices are running with the latest Microsoft security patches. It functions with the Windows probe and Microsoft Baseline Security Analyzer (MBSA 1.2.1) to display the monitored results on the status dashboard for the service. These results help you determine which devices require patch level compliance. Ensuring that the latest patches are installed allows you to protect your Windows devices from viral attacks and security breaches.

The MBSA 1.2.1 software must be installed on the Windows host machine that has the probe installed and set up. The MBSA 1.2.1 must be installed in the default directory suggested by the MBSA installer tool, and the probe must have administrator access to the Windows devices in its domain to monitor them.

The MBSA 1.2.1 service is compatible only with Microsoft Baseline Security Analyzer (MBSA 1.2.1). The system requirements for the MBSA are specified in the Microsoft Knowledge Base article 320454.

Figure 57-1: Monitoring for the Latest Security Patches



Each time the Windows host machine connects to the Internet, the latest MBSA mssecure.xml file is downloaded from the Microsoft Web site. The mssecure.xml file contains information about the latest security patches and their severity levels. Using this file, the MBSA determines the level of compliance of the existing patches on the monitored Windows devices. The MBSA records the data it receives in a log file, which the probe reads and then reports to the N-central server.

For each monitored device, the N-central server compares the information it receives from the probe to the specified regular expressions and thresholds. The appropriate status is then displayed on the Security Services dashboard. The MBSA 1.2.1 scan time, regular expressions and thresholds, and other parameters must be set up by the SO Admin or Admin.

Service Details

Each default keyword is a severity level that is obtained from the MBSA text file and mapped to a regular expression in N-central. For information about these MBSA keywords, refer to the MBSA documentation.

Service Detail	Description
Monitoring	The status of the service: • Enabled, which begins the immediate monitoring of the service on the device. • Disabled, which prevents monitoring of the service on the device. When you would like to temporarily stop the monitoring process, disable the service rather than deleting the service
Time to Stale	The time (in minutes) for the most recent monitored data to become stale. The value must be greater than or equal to the Scan Interval value. Otherwise, the service will be constantly in the Stale state
Monitoring Probe	The central server, probe, or local agent that is being used to monitor the service.
Service Description	A description of the service.
Timeout Value	The time (in seconds) that the central server waits before considering the test a failure.
Start Time	The start hour of a log file scan. The service starts scanning at the specified Start Hour and continues scanning until the end of the End Hour at time intervals specified for Scan Interval in Minutes. For example, if you choose 01:00 as the Start Hour, 02:00 as the End Hour, and 30 as the Scan Interval in Minutes, the service will scan at 1:00, 1:30, 2:00, and 2:30.

Service Detail	Description
End Time	The end hour of a log file scan. The service scans from the specified Start Hour until the end of the specified End Hour at time intervals specified for Scan Interval in Minutes. For example, if you choose 01:00 as the Start Hour, 02:00 as the End Hour, and 30 as the Scan Interval in Minutes, the service will scan at 1:00, 1:30, 2:00, and 2:30. The End Hour is the last hour in which the service will scan, not the cut-off time for the scan.
Scan Interval	The time (in minutes) between each scan.
Repeat Weekly on Day(s)	The log file scan is repeated weekly on the specified days. If you do not select this option but do select an option for the other Scan details, N-central scans continuously.
Repeat Monthly on Day(s)	The log file scan is repeated monthly on the specified days. If you do not select this option but do select an option for the other scan details, N-central scans continuously.
Regular Expression 1-6	The strings of characters and metacharacters that you would like to use to find predetermined key words in the log file(s). You can set a different threshold option for each regular expression.
SUS server	The IP or FQDN of the SUS server at which to check for approved security updates.

Status Details

Status Detail	Default Keyword
Regular Expression 1	Score:.*Severe Risk
Regular Expression 2	Score:.*Potential Risk
Regular Expression 3	Score:.*Incomplete Scan
Regular Expression 4	Score:.*Security FYIs
Regular Expression 5	Score:.*Check Not Performed
Regular Expression 6	Score:.*Additional Information

Chapter 58

MBSA 2.0

Service Type:	Security
Collection Method:	WMI Workstation and MBSA
Instances on a Device:	Single
Supported Platforms:	Microsoft® Windows®
Device Class:	Windows Server and Windows Workstation
Monitored By:	Network Windows Probe, Workgroup - Windows probe **Note:** Network Windows probes are not available in N-central OnDemand
Service Version:	N-central 6.0 and greater

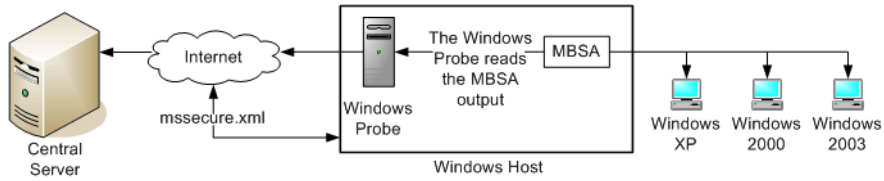
Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* published by Microsoft®.

The MBSA 2.0 service ensures that your Windows devices are running with the latest Microsoft security patches. It functions with the Windows probe and Microsoft Baseline Security Analyzer (MBSA 2.0) to display the monitored results on the status dashboard for the service. These results help you determine which devices require patch level compliance. Ensuring that the latest patches are installed allows you to protect your Windows devices from viral attacks and security breaches.

The MBSA 2.0 software must be installed on the Windows host machine that has the probe installed and set up. The MBSA 2.0 must be installed in the default directory suggested by the MBSA 2.0 installer tool, and the probe must have administrator access to the Windows devices in its domain to monitor them.

The MBSA 2.0 service is compatible with only Microsoft Baseline Security Analyzer (MBSA 2.0).

Figure 58-1: Monitoring for the Latest Security Patches



For each monitored device, the N-central server compares the information it receives from the probe to the specified regular expressions and thresholds. The appropriate status is then displayed on the SecurityServices dashboard. The MBSA 2.0 scan time, regular expressions and thresholds, and other parameters must be set up by the SO Admin or Admin.

Service Details

Each default keyword is a severity level that is obtained from the MBSA text file and mapped to a regular expression in N-central. For information about these MBSA keywords, refer to the MBSA documentation.

Service Detail	Description
Monitoring	The status of the service: • Enabled, which begins the immediate monitoring of the service on the device. • Disabled, which prevents monitoring of the service on the device. When you would like to temporarily stop the monitoring process, disable the service rather than deleting the service
Time to Stale	The time (in minutes) for the most recent monitored data to become stale. The value must be greater than or equal to the Scan Interval value. Otherwise, the service will be constantly in the Stale state
Monitoring Probe	The central server, probe, or local agent that is being used to monitor the service.
Service Description	A description of the service.
Timeout Value	The time (in seconds) that the central server waits before considering the test a failure.
Start Time	The start hour of a log file scan. The service starts scanning at the specified Start Hour and continues scanning until the end of the End Hour at time intervals specified for Scan Interval in Minutes. For example, if you choose 01:00 as the Start Hour, 02:00 as the End Hour, and 30 as the Scan Interval in Minutes, the service will scan at 1:00, 1:30, 2:00, and 2:30.
End Time	The end hour of a log file scan. The service scans from the specified Start Hour until the end of the specified End Hour at time intervals specified for Scan Interval in Minutes. For example, if you choose 01:00 as the Start Hour, 02:00 as the End Hour, and 30 as the Scan Interval in Minutes, the service will scan at 1:00, 1:30, 2:00, and 2:30. The End Hour is the last hour in which the service will scan, not the cut-off time for the scan.

Service Detail	Description
Scan Interval	The time (in minutes) between each scan.
Repeat Weekly on Day(s)	The log file scan is repeated weekly on the specified days. If you do not select this option but do select an option for the other Scan details, N-central scans continuously.
Repeat Monthly on Day(s)	The log file scan is repeated monthly on the specified days. If you do not select this option but do select an option for the other scan details, N-central scans continuously.
Regular Expression 1-6	The strings of characters and metacharacters that you would like to use to find predetermined key words in the log file(s). You can set a different threshold option for each regular expression.
MBSA Parameters	Parameters to be used with the Microsoft Baseline Security Analyzer (MBSA).
Executable Path Location	The location where Microsoft Baseleine Security Analyzer (MBSA) was installed.

Status Details

Status Detail	Default Keyword
Regular Expression 1	Score:.*Check failed .*critical
Regular Expression 2	Score:.*Check failed .*non-critical
Regular Expression 3	Score:.*Unable to scan
Regular Expression 4	Score:.*Best practice
Regular Expression 5	Score:.*Check not performed
Regular Expression 6	

Chapter 59

Memory

The Memory services (Local API, Novell SNMP, SNMP, WMI) monitor the used, free, and total space of the physical memory and virtual memory on a device. One instance of this service can monitor all of the detected swap files on multiple volumes. The monitored results are presented in an aggregate value on the status dashboard for the service. The maximum size of a swap file that is monitored by this service is 16GB.

Memory (Cisco) monitors memory pool utilization on any Cisco device using SNMP. The device must be SNMP CISCO -MEMORY- POOL-MIB compliant.

Memory (Local API, Novell SNMP, SNMP, WMI)

Service Type:	System
Collection Method:	Local, Novell, SNMP, and WMI Workstation
Instances on a Device:	Single
Supported Platforms:	N/A
Device Class for Memory (Local API):	Generic Server, Generic Workstation, Windows Server, and Windows Workstation
Device Class for Memory (Novell SNMP):	Generic Server and Generic Workstation
Device Class for Memory (SNMP):	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Device Class for Memory (WMI):	Windows Server and Windows Workstation
Monitored By:	Local API (Windows, Novell Netware, RedHat Linux, RedHat Enterprise Linux, Suse Linux, and Mac OSX 10.4 agents), SNMP (Network Hardware Probe), and WMI (Windows probes)
Service Version:	N-central 5.0 and greater

Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* published by Microsoft®.

Service Details

Common Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	

Memory (SNMP) Service Details

Service Detail	Description
Physical Memory Index	The resulting OID index for the average physical memory used over the last minute for the Memory (SNMP) service. The index values can be obtained by performing an SNMP walk on the OID value: .1.3.6.1.2.1.25.2.3.1.3 (hrStorageDescr). You must determine which OID and index value is relevant. The OID value is contained in the HOST-RESOURCES-MIB definition file.
Physical Memory Name	The string corresponding to the row in the hrStorageTable, which describes the type and instance of the table for the Memory (SNMP) service. The string can be obtained by performing an SNMP walk on the OID value: .1.3.6.1.2.1.25.2.3.1.3 (hrStorageDescr).
Virtual Memory Index	The resulting OID index for the average virtual memory used over the last minute for the Memory (SNMP) service. For more information, refer to the description on Physical Memory Index.
Virtual Memory Name	The string corresponding to the row in the hrStorageTable, which describes the type and instance of the table for the Memory (SNMP) service. The string can be obtained by performing an SNMP walk on the OID value: .1.3.6.1.2.1.25.2.3.1.3 (hrStorageDescr).

SNMP (Novell) Service Details

Service Detail	Description
Free Memory Index	The OID index for free memory for the Memory (Novell SNMP) service. The index values can be obtained by performing an SNMP walk on the OID value: .1.3.6.1.2.1.25.2.3.1.3 (hrStorageDescr).
Free Memory Description	The OID value for free memory for the Memory (Novell SNMP) service. The index values can be obtained by performing an SNMP walk on the OID value: .1.3.6.1.2.1.25.2.3.1.3 (hrStorageDescr).
Used Memory Index	The OID index for used memory for the Memory (Novell SNMP) service. The index values can be obtained by performing an SNMP walk on the OID value: .1.3.6.1.2.1.25.2.3.1.3 (hrStorageDescr).
Used Memory Description	The OID index for used memory. The index values can be obtained by performing an SNMP walk on the OID value: .1.3.6.1.2.1.25.2.3.1.3 (hrStorageDescr).

Status Details

Memory Status Details

Status Detail	Description
Physical Memory Usage (%)	The percentage of physical memory used. This percentage is compared to the thresholds.
Virtual Memory Usage (%)	The percentage of virtual memory used. This percentage is compared to the thresholds.

Memory (Cisco)

Service Type: Network
Collection Method: SNMP
Instances on a Device: Single
Supported Platforms: N/A
Device Class: Switch/Router
Monitored By: SNMP (Network Hardware Probe)
Service Version: N-central 5.0 and greater

Service Details

Memory (Cisco) Service Details

Service Detail	Description
Monitoring	Refer to .
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Cisco Memory Pool Name Index	The index of the textual name assigned to the memory pool, which is determined by performing an SNMP walk on ciscoMemoryPoolName (.1.3.6.1.4.1.9.9.48.1.1.1.2).
Cisco Memory Pool Name Value	The value of the textual name assigned to the memory pool, which is determined by performing an SNMP walk on ciscoMemoryPoolName (.1.3.6.1.4.1.9.9.48.1.1.1.2).

Status Details

Memory (Cisco) Status Details

Status Detail	Description
Name	The name of the memory pool being monitored.
Used	The amount of used memory.
Free	The amount of free memory.

Status Detail	Description
Total	The total memory for that memory pool.
% Memory Utilization	The utilization of memory as a percentage of the whole amount of available memory.

Chapter 60
NNTP

Service Type:	Network
Collection Method:	TCP
Instances on a Device:	Single
Supported Platforms:	N/A
Device Class:	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server
Service Version:	N-central 3.0 and greater

The Network News Transfer Protocol (NNTP) test checks the status of the NNTP process on the network device. NNTP is a request-reply protocol that is similar in style to the Simple Mail Transfer Protocol (SMTP) or FTP. It provides a network news transport service and is the standard for the Internet exchange of Usenet messages.

N-central can determine the up or down status of the NNTP service. The NNTP service does not use the Warning state.

N-central averages the availability of the NNTP service over the scan interval. It compares the availability of the NNTP service to the threshold to determine the status.

Service Details

NNTP Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Time Out Value	
Port Number	
Validating String	

Status Details

NNTP Status Details

Status Detail	Description
NNTP Service Availability	N-central determines whether the NNTP service is up or down. The NNTP service does not use the Warning state. N-central averages the availability of the NNTP service over the scan interval and compares the availability of the NNTP service to the threshold to determine the status.
Round Trip Time (ms)	The time (in milliseconds) for a request to be sent and received.
DNS Resolution	The threshold that determines whether the device name can be resolved. If an FQDN has been specified, the service searches for its IP address. If the IP address is found, the state will be Normal. Otherwise, it will be Failed, based on the default settings. If an IP address has been specified, the service checks only the IP address's format. If the format is correct, the state will be Normal. Otherwise, it will be Failed, based on the default settings.

Chapter 61
POP

Service Type: Network

Collection Method: TCP

Instances on a Device: Single

Supported Platforms: N/A

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server

Service Version: N-central 3.0 and greater

N-central can monitor a network device for the presence of a Post Office Protocol, version 3 (POP 3) mail server that is available to the network. POP 3 is a protocol designed for user-to-mailbox access. It is used on the Internet to retrieve email from a mail server.

N-central can determine the up or down status of the POP service. The POP service does not use the Warning state. N-central averages the availability of the POP service over the scan interval. It compares the availability of the POP service to the threshold to determine the status.

Service Details

POP Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Timeout Value	
Port Number	
Validating String	

Status Details

POP Status Details

Status Detail	Description
POP Service Availability	N-central determines whether the POP service is up or down. The POP service does not use the Warning state. N-central averages the availability of the POP service over the scan interval and compares the availability of the POP service to the threshold to determine the status.
Round Trip Time (ms)	The time (in milliseconds) for a request to be sent and received.
DNS Resolution	The threshold that determines whether the device name can be resolved. If an FQDN has been specified, the service searches for its IP address. If the IP address is found, the state will be Normal. Otherwise, it will be Failed, based on the default settings. If an IP address has been specified, the service checks only the IP address's format. If the format is correct, the state will be Normal. Otherwise, it will be Failed, based on the default settings.

Chapter 62

Patch Management

Service Type:	WSUS
Collection Method:	N-able Connector
Instances on a Device:	Single
Supported Platforms:	WSUS 2.0 and WSUS 3.0 Beta 2
Device Class:	Windows Server and Windows Workstation
Monitored By:	Central Server
Service Version:	N-central 6.0 and greater

The Patch Management service monitors devices to determine whether or not required updates and patches have been installed.

This service is only available for Windows devices that have been configured on the WSUS server. Please note, N-central must be configured to interact with WSUS. For more information, refer to Configuring N-central for Patch Management.

Service Details

Detail	Description
Monitoring	The status of the service: • Enabled, which begins the immediate monitoring of the service on the device. • Disabled, which prevents monitoring of the service on the device. When you would like to temporarily stop the monitoring process, disable the service rather than deleting the service.
Time to Stale	The time (in minutes) for the most recent monitored data to become Stale. The value must be greater than or equal to the Scan Interval value. Otherwise, the service will be constantly in the Stale state.
Current Monitoring Probe	The central server that is being used to monitor the service.
Service Description	A description of the service.
Scan Interval	The time (in minutes) between each scan.
Timeout Value	The time (in seconds) that the central server waits before considering the test a failure.

Status Details

Status Detail	Description
Patch Compliance	The status of a device's patch compliance. If the device does not have all of the required updates or patches installed, a value of False is returned. If the device has all the required updates or patches installed, a value of True is returned.
Missing Patch Count (Patches)	The total number of required updates and patches that have not been installed on the device.
Missing Patches	A list of all the required updates and patches that have not been installed on the device.

Chapter 63

Power Supply

Power Supply (Dell)

Service Type: Network

Collection Method: SNMP

Instances on a Device: Multiple

Supported Platforms: Dell PowerEdge series servers running Dell OpenManage Server Administrator software

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Hardware Probe, Windows Probes

Service Version: N-central 5.0 and greater

The Power Supply (Dell) service monitors the overall condition of the power supply sub-system for Dell servers.

Service Details

Power Supply (Dell) Service Details

Service Detail	Description
Monitoring	Refer to .
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	
Power Supply Location Index	The index of the location name of the power supply, which is determined by performing an SNMP walk on powerSupplyLocationName (.1.3.6.1.4.1.674.10892.1.600.12.1.8).
Power Supply Location Value	The string of the location name of the power supply, which is determined by performing an SNMP walk on powerSupplyLocationName (.1.3.6.1.4.1.674.10892.1.600.12.1.8).

Configuring Power Supply Location Index or Value

To configure Power Supply Location Index or Location Value,

You will have to walk the OID .1.3.6.1.4.1.674.10892.1.600.12.1.8 and look at the results.

Example:

snmpwalk -Cp -On -c public -v1 10.20.30.29 \ .1.3.6.1.4.1.674.10892.1.600.12.1.8

```
.1.3.6.1.4.1.674.10892.1.600.12.1.8.1.1 = STRING: "Power
Supply 1"
.1.3.6.1.4.1.674.10892.1.600.12.1.8.1.2 = STRING: "Power
Supply 2"
Variables found: 2
```

In this case, there are two power supplies, their indices are “1.1” and “1.2”. To monitor both power supplies, add the service twice. Enter “1.1” for the Power Supply Location Index or “Power Supply 1” for the Power Supply Location Value for the first task. Then add “1.2” as the index or “Power Supply 2” as the value for the second task.

Status Details

Power Supply (Dell) Status Details

Scan Details	Description
Power Supply (Dell) Status	The status of the power supply.

Power Supply (HP)

Service Type: Network

Collection Method: SNMP

Instances on a Device: Single

Supported Platforms: Compaq/HP ProLiant Series Servers running Compaq Insight Manager v7

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Hardware Probe, Windows Probes

Service Version: N-central 5.0 and greater

The Power Supply (HP) service monitors the overall condition of the power supply sub-system for Compaq/HP ProLiant servers.

Service Details

Power Supply (HP) Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	

Status Details

Power Supply (HP) Service Details

Status Detail	Description
Power Supply (HP)	The overall condition of the fault tolerant power supply sub-system.

Chapter 64
Printer

Printer services allow you to monitor the status of your printer's:

- paper supply,
- toner levels, and
- page count.

Printer services also generate notifications and trend reports on your printer's availability. Printer services monitor any SNMP Printer-MIB Compliant Device (RFC1759).

Paper Supply Level

Service Type: Network

Collection Method: SNMP

Instances on a Device: Multiple

Supported Platforms: Any SNMP Printer-MIB Compliant Device (RFC1759)

Device Class: Printer

Monitored By: Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe

Service Version: N-central 5.0 and greater

The Paper Supply Level service monitors the amount of paper as a percentage of the total capacity of the printer. The printers monitored by this service include any printer that is an SNMP Printer-MIB Compliant Device (RFC1759) and reports paper supply level.

Service Details

Paper Supply Level Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	

Service Detail	Description
Printer Input Description Index	The index for the prtInputDescription object, which is determined by performing an SNMP walk on the prtInputTable table and locating prtInputDescription (.1.3.6.1.2.1.43.8.2.1.18.).
Printer Input Description Value	The description for the prtInputDescription object, which is determined by performing an SNMP walk on the prtInputTable table and locating prtInputDescription (.1.3.6.1.2.1.43.8.2.1.18).

Configuring Printer Input Description Index or Description Value

To configure Printer Input Description Index or Description Value

Walk the OID “1.3.6.1.2.1.43.8.2” on the target device address to determine which indices are available for monitoring.

Example:

```
.1.3.6.1.2.1.43.8.2.1.9.1.1  100
.1.3.6.1.2.1.43.8.2.1.9.1.2  500
.1.3.6.1.2.1.43.8.2.1.9.1.3  500
.1.3.6.1.2.1.43.8.2.1.10.1.1 0
.1.3.6.1.2.1.43.8.2.1.10.1.2 -3
.1.3.6.1.2.1.43.8.2.1.10.1.3 -3
.1.3.6.1.2.1.43.8.2.1.18.1.1 "Tray 1"
.1.3.6.1.2.1.43.8.2.1.18.1.2 "Tray 2"
.1.3.6.1.2.1.43.8.2.1.18.1.3 "Tray 3"
```

Substituting the numerical object identifiers with their textual representations, the walk becomes:

```
prtInputMaxCapacity.1.1  100
prtInputMaxCapacity.1.2  500
prtInputMaxCapacity.1.3  500
prtInputCurrentLevel.1.1 0
prtInputCurrentLevel.1.2 -3
prtInputCurrentLevel.1.3 -3
prtInputDescription.1.1  "Tray 1"
prtInputDescription.1.2  "Tray 2"
prtInputDescription.1.3  "Tray 3"
```

There are three indices in this case - "1.1", "1.2" and "1.3". Only "1.1" is relevant because the other entries in prtInputCurrentLevel are –3, which means they cannot be accurately measured according to the MIB description.

Status Details

Paper Supply Level Status Details

Status Detail	Description
Description	A free-form text description of the input sub-unit.
Max Capacity	The maximum capacity of the input sub-unit in input sub-unit capacity units.
Level	The current capacity of the input sub-unit in input sub-unit capacity units.
Paper Level (%)	A calculated percentage of the utilization of the input sub-unit.

Printer Conf Changes

Service Type: Network

Collection Method: SNMP

Instances on a Device: Single

Supported Platforms: Any SNMP Printer-MIB Compliant Device (RFC1759).

Device Class: Printer

Monitored By: Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe

Service Version: N-central 6.0 and greater

The Printer Conf service monitors the number of configuration changes that affect the capabilities of a printer such as the addition or deletion of input/output bins, the addition or deletion of print interpreters, or modifications to the media size. These changes can often affect the ability of the printer to service specific types of print jobs.

Printer management applications may cache configuration information about sub-units on the printer that is modified infrequently. This will be incremented whenever the agent instructs applications to invalidate the cache and download all of the configuration information once again. This indicates a change in the printer's configuration.

Service Detail

Printer Conf Changes Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	

Configuring Printer Conf Changes

Walk the OIDs on the target device's SNMP agent to determine which indices are available for monitoring.

Example:

```
.1.3.6.1.2.1.43.5.1.1.1 1984
```

Substituting the OIDs with the MIBs the walk becomes:

```
prtGeneralConfigChanges.1 1984
```

There is one index in this case - "1".

```
Printer Conf Changes #1
prtGeneralConfigChanges Index = "1"
```

Status Details

Printer Conf Changes Status Details

Status Details	Description
Printer Conf Changes	A numeric counter indicating the number of configuration changes that have been applied to the target printer.

Printer Cover Status

Service Type: Network

Collection Method: SNMP

Instances on a Device: Single

Supported Platforms: Any SNMP Printer-MIB Compliant Device (RFC1759).

Device Class: Printer

Monitored By: Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe

Service Version: N-central 6.0 and greater

The Printer Cover Status service monitors the current status of the printer cover.

Service Detail

Printer Cover Status Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	

Configuring the Printer Cover Status

Walk the OIDs on the target device's SNMP agent to determine which indices are available for monitoring.

Example:

```
.1.3.6.1.2.1.43.6.1.1.2.1.1 ""
.1.3.6.1.2.1.43.6.1.1.3.1.1 4
```

Substituting the OIDs with the MIBs the walk becomes:

```
prtCoverDescription.1.1 4
prtCoverStatus.1.1      4
```

There is one index in this case - "1.1".

```
Printer Cover Status #1
prtCoverDescription Index = "1.1"
prtCoverStatus Index      = "1.1"
```

Status Details

Printer Cover Status Status Details

Status Details	Description
Printer Cover Description	The name of the cover sub-mechanism provided by the manufacturer.
Printer Cover Status	Indicates the current condition of the printer cover as one of the following: • **Normal** - the printer cover is closed and the device can function normally. • **Warning** - the printer cover may be open or partially open preventing the device from functioning normally. • **Failed** - the printer cover is open preventing the device from functioning normally.

Printer Display

Service Type: Network

Collection Method: SNMP

Instances on a Device: Multiple

Supported Platforms: Any printer that reports the contents of its display via the Printer-MIB.

Device Class: Printer

Monitored By: Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe

Service Version: N-central 6.0 and greater

The Printer Display service monitors the content of the line of text contained in the logical display buffer of the operator's console for the printer.

Service Detail

Printer Display Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	

Configuring the Printer Display Service

Use an snmp tool to walk the object id you wish to monitor and get the index.

Example:

```
# snmpwalk -On -c public -v1 hp-printer.engineering.n-able.com .1.3.6.1.2.1.43.16.5.1.2
.1.3.6.1.2.1.43.16.5.1.2.1.1 = STRING: "Ready"
.1.3.6.1.2.1.43.16.5.1.2.1.2 = ""
.1.3.6.1.2.1.43.16.5.1.2.1.3 = STRING: "To enter menus"
.1.3.6.1.2.1.43.16.5.1.2.1.4 = Hex-STRING: 70 72 65 73 73 20 1E
.1.3.6.1.2.1.43.16.5.1.2.1.5 = ""
.1.3.6.1.2.1.43.16.5.1.2.1.6 = ""
.1.3.6.1.2.1.43.16.5.1.2.1.7 = ""
.1.3.6.1.2.1.43.16.5.1.2.1.8 = ""
.1.3.6.1.2.1.43.16.5.1.2.1.9 = ""
.1.3.6.1.2.1.43.16.5.1.2.1.10 = ""
.1.3.6.1.2.1.43.16.5.1.2.1.11 = ""
```

```
.1.3.6.1.2.1.43.16.5.1.2.1.12 = ""
```

Substituting the numerical OIDs with their textual equivalents, the walk becomes:

```
prtConsoleDisplayBufferText.1.1 = STRING: "Ready"
prtConsoleDisplayBufferText.1.2 = ""
prtConsoleDisplayBufferText.1.3 = STRING: "To enter menus"
prtConsoleDisplayBufferText.1.4 = Hex-STRING: 70 72 65 73 73
20 1E
prtConsoleDisplayBufferText.1.5 = ""
prtConsoleDisplayBufferText.1.6 = ""
prtConsoleDisplayBufferText.1.7 = ""
prtConsoleDisplayBufferText.1.8 = ""
prtConsoleDisplayBufferText.1.9 = ""
prtConsoleDisplayBufferText.1.10 = ""
prtConsoleDisplayBufferText.1.11 = ""
prtConsoleDisplayBufferText.1.12 = ""
```

In this case, the service should be added 12 times, entering the indices of 1.1 through to 1.12.

Status Details

Printer Display Status Details

Status Details	Description
Display Text	The text currently being shown in the printer's console display.
System Uptime	The time that has passed since the printer was last turned on or restarted.

Printer Page Count

Service Type: Network

Collection Method: SNMP

Instances on a Device: Multiple

Supported Platforms: Any SNMP Printer-MIB Compliant Device (RFC1759)

Device Class: Printer

Monitored By: Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe

Service Version: N-central 5.0 and greater

The Printer Page Count service monitors the count of pages for the lifetime of the printer and the count of pages since the last time the printer was turned on.

Service Detail

Printer Page Count Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Printer Marker Index	The index of the printer device and sub-unit, which is determined by performing an SNMP walk on prtMarkerLifeCount (.1.3.6.1.2.1.43.10.2.1.4).

Configuring the Printer Marker Index

Walk the OID .1.3.6.1.2.1.43.10.2 on the target device to determine which indices are available for monitoring.

Example:

```
.1.3.6.1.2.1.43.10.2.1.4.1.1 1158
.1.3.6.1.2.1.43.10.2.1.5.1.1 1158
```

Substituting the numerical object ids with their textual representations, the walk becomes:

```
prtMarkerLifeCount.1.1    1158
prtMarkerPowerOnCount.1.1 1158
```

There is one index in this case— "1.1".

Status Details

Printer Page Count Status Details

Status Details	Description
Page Count	Typically, this is the count of pages printed for the lifetime of the equipment. More accurately, this is the count of units of measure printed for the lifetime of the equipment.
Power On Count	Typically, this is the count of pages printed since the equipment was most recently powered on. More accurately, this is the count of units of measure printed since the equipment was most recently powered on.

Printer Page Count (HP)

Service Type: Network

Collection Method: SNMP

Instances on a Device:	Single
Supported Platforms:	Any HP printer which supports the Printer-MIB (RFC1759) and the CLJ8500-MIB HP private mib.
Device Class:	Printer
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe
Service Version:	N-central 6.0 and greater

The Printer Page Count (HP) service monitors the count of pages (including a total count as well as color and black-and-white) for the lifetime of an HP printer.

Service Detail

Printer Page Count (HP) Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Printer Marker Index	The index of the printer device and sub-unit, which is determined by performing an SNMP walk on prtMarkerLifeCount (.1.3.6.1.2.1.43.10.2.1.4).

Configuring the Printer Marker Index

Walk the OID on the target device's SNMP agent to determine which indices are available for monitoring.

Example:

```
snmpwalk -On -c public -v 2c 10.150.1.46
.1.3.6.1.2.1.43.10.2.1.4
```

```
.1.3.6.1.2.1.43.10.2.1.4.1.1 = Counter32: 258499
```

There is one index in this case - "1.1".

The HP private OID, total-color-page-count, must also be reported by the printer. It's index is always 0.

```
snmpwalk -On -c public -v 2c 10.150.1.46
.1.3.6.1.4.1.11.2.3.9.4.2.1.4.1.2.7
```

```
.1.3.6.1.4.1.11.2.3.9.4.2.1.4.1.2.7.0 = INTEGER: 14
```

Status Details

Printer Page Count (HP) Status Details

Status Details	Description
Total Page Count	Typically, this is the count of pages printed for the lifetime of the equipment. More accurately, this is the count of units of measure printed for the lifetime of the equipment.
Color Page Count	Typically, this is the count of pages printed in color for the lifetime of the equipment. More accurately, this is the count of units of measure printed in color for the lifetime of the equipment.
Black and White Page Count	Typically, this is the count of pages printed in black-and-white for the lifetime of the equipment. More accurately, this is the count of units of measure printed in black-and-white for the lifetime of the equipment.

Printer Serial Number

Service Type: Network

Collection Method: SNMP

Instances on a Device: Multiple

Supported Platforms: Any printer that reports its serial number via the Printer-MIB v2.

Device Class: Printer

Monitored By: Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe

Service Version: N-central 6.0 and greater

The Printer Serial Number service monitors a recorded serial number for a specified printer used in reference with a device catalog or inventory.

Service Detail

Printer Serial Number Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	

Configuring the Printer Serial Number Service

Use an snmp tool to walk the object id you wish to monitor and get the index.

Example:

```
        # snmpwalk -On -c public -v1 hp-
printer.engineering.n-able.com .1.3.6.1.2.1.43.5.1.1.17
.1.3.6.1.2.1.43.5.1.1.17.1 = STRING: "USBNX05830"
```

Substituting the numerical OIDs with their textual equivalents, the walk becomes:

```
prtGeneralSerialNumber.1 = STRING: "USBNX05830"
```

In this case, the index is 1.

Status Details

Printer Serial Number Status Details

Status Details	Description
General Serial Number	The serial number of the target printer.
System Uptime	The time that has passed since the printer was last turned on or restarted.

Printer Status

Service Type: Network

Collection Method: SNMP

Instances on a Device: Single

Supported Platforms: Any SNMP HOST-RESOURCES-MIB Compliant Device (RFC1514).

Device Class: Printer

Monitored By: Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe

Service Version: N-central 6.0 and greater

The Printer Status service monitors the current status of a specified printer.

Service Detail

Printer Status Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	

Configuring the Printer Status Service

Walk the OIDs on the target device's SNMP agent to determine which indices are available for monitoring.

Example:

```
.1.3.6.1.2.1.25.3.5.1.1.1 3
.1.3.6.1.2.1.25.3.5.1.2.2 2
.1.3.6.1.2.1.25.3.5.1.1.1 80
.1.3.6.1.2.1.25.3.5.1.2.2 80
```

Substituting the OIDs with the MIBs the walk becomes:

```
hrPrinterStatus.1             3
hrPrinterStatus.2             2
hrPrinterDetectedErrorState.1 80
hrPrinterDetectedErrorState.2 80
```

There are two indices in this case - "1" and "2".

Printer Status #1

```
Printer Status Instance ID                = "1"
Printer Detected Error State Instance ID = "1"
```

Printer Status #2

```
Printer Detected Error State Instance ID = "2"
Printer Detected Error State Instance ID = "2"
```

Status Details

Printer Status - Status Details

Status Details	Description
Printer Status	Indicates the current condition of the printer as one of the following: • **Normal** - the printer is functioning normally. • **Warning** - the printer may be experiencing problems preventing it from functioning normally. • **Failed** - the printer is not functioning normally.
Printer Detected Error State	If the printer is in an error state, the conditions that defined this state are reported as one of the following: • Low supply of paper, • No paper available, • Low supply of toner, • No toner available, • A door on the printer is open, • The printer is jammed, • The printer is offline, • Technical service is requested for the printer, • The input tray is missing or not installed properly, • The output tray is missing or not installed properly, • The marker supply is missing or not installed properly, • The output tray is nearly full, • The output tray is full, • The input tray is empty, or, • The printer is overdue for preventative maintenance.

Printer Toner Level

Service Type: Network

Collection Method: SNMP

Instances on a Device: Multiple

Supported Platforms: Any SNMP Printer-MIB Compliant Device (RFC1759)

Device Class: Printer

Monitored By: Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe

Service Version: N-central 5.0 and greater

The Printer Toner Level service monitors the amount of toner as a percentage of the total capacity of the monitored printer.

Service Details

Printer Toner Level Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Printer Marker Supplies Description Index	The index of the printer device and marker supply, which is determined by performing an SNMP walk on prtMarkerSuppliesDescription (.1.3.6.1.2.1.43.11.1.1.6).
Print Marker Supplies Description Value	The description value for the marker supply, which is determined by performing an SNMP walk on prtMarkerSuppliesDescription (.1.3.6.1.2.1.43.11.1.1.6).

Configuring Print Marker Supplies Description Index or Value

To configure the Print Marker Supplies Description Index or Value

Walk the object id .1.3.6.1.2.1.43.11.1 on the target device's address to determine which indices or descriptions are available for monitoring.

Example:

```
.1.3.6.1.2.1.43.11.1.1.6.1.1 "Black Toner"
.1.3.6.1.2.1.43.11.1.1.6.1.2 "Cyan Toner"
.1.3.6.1.2.1.43.11.1.1.6.1.3 "Magenta Toner"
.1.3.6.1.2.1.43.11.1.1.6.1.4 "Yellow Toner"
.1.3.6.1.2.1.43.11.1.1.6.1.5 "Fuser"
.1.3.6.1.2.1.43.11.1.1.6.1.6 "Transfer Roller"
.1.3.6.1.2.1.43.11.1.1.6.1.7 "Coating Roller"
.1.3.6.1.2.1.43.11.1.1.8.1.1 10000
.1.3.6.1.2.1.43.11.1.1.8.1.2 10000
.1.3.6.1.2.1.43.11.1.1.8.1.3 10000
.1.3.6.1.2.1.43.11.1.1.8.1.4 10000
.1.3.6.1.2.1.43.11.1.1.8.1.5 100000
.1.3.6.1.2.1.43.11.1.1.8.1.6 -2
.1.3.6.1.2.1.43.11.1.1.8.1.7 21000
.1.3.6.1.2.1.43.11.1.1.9.1.1 3300
```

```
.1.3.6.1.2.1.43.11.1.1.9.1.2 9600
.1.3.6.1.2.1.43.11.1.1.9.1.3 9700
.1.3.6.1.2.1.43.11.1.1.9.1.4 9800
.1.3.6.1.2.1.43.11.1.1.9.1.5 -3
.1.3.6.1.2.1.43.11.1.1.9.1.6 -3
.1.3.6.1.2.1.43.11.1.1.9.1.7 -3
```

Substituting the numerical object ids for their textual representations, the walk becomes:

```
prtMarkerSuppliesDescription.1.1 "Black Toner"
prtMarkerSuppliesDescription.1.2 "Cyan Toner"
prtMarkerSuppliesDescription.1.3 "Maganta Toner"
prtMarkerSuppliesDescription.1.4 "Yellow Toner"
prtMarkerSuppliesDescription.1.5 "Fuser"
prtMarkerSuppliesDescription.1.6 "Transfer Roller"
prtMarkerSuppliesDescription.1.7 "Coating Roller"
prtMarkerSuppliesMaxCapacity.1.1 10000
prtMarkerSuppliesMaxCapacity.1.2 10000
prtMarkerSuppliesMaxCapacity.1.3 10000
prtMarkerSuppliesMaxCapacity.1.4 10000
prtMarkerSuppliesMaxCapacity.1.5 100000
prtMarkerSuppliesMaxCapacity.1.6 -2
prtMarkerSuppliesMaxCapacity.1.7 21000
prtMarkerSuppliesLevel.1.1       3300
prtMarkerSuppliesLevel.1.2       9600
prtMarkerSuppliesLevel.1.3       9700
prtMarkerSuppliesLevel.1.4       9800
prtMarkerSuppliesLevel.1.5       -3
prtMarkerSuppliesLevel.1.6       -3
prtMarkerSuppliesLevel.1.7       -3
```

There are seven indices in this case— "1.1", "1.2", "1.3", "1.4", "1.5", "1.6" and "1.7". For the first marker supply, you may enter “1.1” or “Black Toner”.

Status Details

Printer Toner Level Status Details

Status Detail	Description
Description	The description of this supply container or receptacle.
Max Capacity	The maximum capacity of this supply container or receptacle expressed in supply units.

Status Detail	Description
Level	The current level if this supply is a container; the remaining space if this supply is a receptacle.
Toner Level	A calculated utilization of the container or receptacle. Canon printers may not report toner level in a usable fashion. The Max Capacity is reported as 2; therefore, the Level can be 0, 1, or 2. This results in the Toner Level (%) calculation becoming 0%, 50% or 100%.

Chapter 65

Probe Status

Service Type: System

Collection Method: Central Server Asset

Instances on a Probe: Single

Supported Platforms: Hardware Probe, Workgroup Windows Probe, and Network Windows Probe

Device Class: N/A

Monitored By: Central Server Asset

Service Version: N-central 6.0 and greater

The Probe Status service monitors the time since the probe last checked in.

When Probe Status is first added to a device, the service will be in a Misconfigured state until the probe first makes contact with the central server.

During the monitoring process, the central server queries the time of the most recent connection of the probe to the central server. This is compared to the current time and the resulting difference is then compared to the specified threshold values so that it can be represented by the appropriate state on the status dashboard for the service.

Example: If the time difference between the previous and current connection is within 10 minutes, the service state will display Normal; between 10 and 20 minutes, Warning; and over 20 minutes, Failed.

Service Details

Probe Status Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	

Status Details

Probe Status Details

Status Detail	Description
Check-In Interval	The threshold that compares the time difference between the current time and the most recent connection to the specified threshold values.

Chapter 66

Process

Service Type:	System
Collection Method:	Local API, SNMP, and WMI Workstation
Instances on a Device:	Multiple
Supported Platforms:	N/A
Device Class for Process (Local API):	Generic Server, Generic Workstation, Windows Server, and Windows Workstation
Device Class for Process (SNMP):	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Device Class for Process (WMI):	Windows Server and Windows Workstation
Monitored By:	Agent (Windows, Novell Netware, RedHat Linux, RedHat Enterprise Linux, Suse Linux, and Mac OSX 10.4)
Service Version:	N-central 3.0 and greater

Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* published by Microsoft®.

The Process service monitors Windows services as well as Linux and Novell processes. A maximum of ten services or processes can be monitored on each Windows device.

During the monitoring process, the availability of the service is averaged over the scan interval. The result is then compared to the specified thresholds to determine the up or down state of the service.

Note: The Process (Local API) and Process (WMI) services do not use the Warning state.

Service Detail

Process (Local API, SNMP, and WMI) Service Details

Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	
Process Index	The resulting OID index for the status of running processes over the last minute for the Process (SNMP) service. The index values can be obtained by performing an SNMP walk on the OID value: .1.3.6.1.2.1.25.4.2.1.2 (hrSWRunName). The index values are: .1, .8, .164, .192, .212, .240, .252, .420, .448, .512, .544, .564, .576, .628, .692, .708, .740, .800, .868, .900, .972, .1016, .1032, .1060, .1084, .1212, .1256, .1792, and .1800. Only a maximum of 10 values can be monitored. You must determine which OID index value is relevant. The OID description is contained in the HOST-RESOURCES-MIB definition file.
Process Name	The name of the process to monitor. If the Process service is monitored by a Windows probe, the name must match the executable name that is listed in the Processes tab of the Windows Task Manager, must include the file extension, and must be specified within double quotation marks. Example: “IEXPLORER.EXE” For the Process (SNMP) service, the name must match the OID value: .1.3.6.1.2.1.25.4.2.1.2 (hrSWRunName).
Process PID File (Linux Only)	The directory path of the process identification (PID) number file. The PID file is used for Linux (Local API) agents only. To avoid generating an unnecessary Failed status for this service, ensure that you provide access to: • the directory in which the PID file is located, and • the PID file itself.

Status Details

Process (Local API, SNMP, and WMI) Status Details

Status Detail	Description
Process Availability	The availability of the Process service. The threshold values that determine the up or down state of the service.
The Number of Process Instances	The number of instances of a process to monitor for the Process (WMI) service. The status of the process to monitor for the Process (Local API) and Process (SNMP) services.

Chapter 67

Security Logs

Service Type: Security

Collection Method: Syslog

Instances on a Device: Single

Supported Platforms: N/A

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Network Hardware Probe, Network Windows Probe, and Workgroup Windows Probe

Service Version: N-central 3.0 SP3 and greater

This service monitors the SNMP traps and syslog messages that are transmitted to the monitoring probe. Appliances and applications that run on a computer, such as a server, can be configured to record events to the probe.

During the monitoring process, this service listens for SNMP traps and log messages that are transmitted to the probe. The service then interprets these events and displays the appropriate status based on the regular expressions that you define. The service also supports wide characters.

Service Details

Security Logs Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Service Description	
Scan Interval	
Regular Expressions 1 to 6	

Status Details

Security Logs Status Details

Status Detail	Description
Regular Expressions (1 to 6)	The threshold values for the regular expressions that you specified on the Service Details tab.
The line count matched regex...	The number of lines, in the log file, on which the keyword has been located and returned by the agent. This information is displayed for each regular expression on the status details screen for the service, any applicable reports, and any triggered notifications (except for numeric pages).
The first line matched	The first 250 characters of the first line, in the log file, containing the matching keyword returned by the agent. This information is displayed on the service's status details screen, any applicable reports, and any triggered notifications (except for numeric pages).

Chapter 68

Server Temp

Server Temp (Dell)

Service Type: Network

Collection Method: SNMP

Instances on a Device: Multiple

Supported Platforms: Dell PowerEdge series servers running Dell OpenManage Server Administrator software

Device Class: Generic Server, Other, Printer, Scanner/Camera, Switch/Router, Windows Server

Monitored By: Hardware Probe, Windows Probes

Service Version: N-central 5.0 and greater

The Server Temp (Dell) service monitors the overall condition of the system's thermal environment for Dell servers.

Service Details

Server Temp (Dell) Service Details

Service Detail	Description
Monitoring	Refer to .
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	
Temperature Probe Location Name Index	The index of the location name of the temperature probe, which is determined by performing an SNMP walk on temperatureProbeLocationName (.1.3.6.1.4.1.674.10892.1.700.20.1.8).
Temperature Probe Location Name Value	The string of the location name of the temperature probe, which is determined by performing an SNMP walk on temperatureProbeLocationName (.1.3.6.1.4.1.674.10892.1.700.20.1.8).

Configuring Temperature Probe Location Name Index or Value

To configure Temperature Probe Location Name Index or Value

Walk the object ID .1.3.6.1.4.1.674.10892.1.700.20.1.8 with an SNMP client and look at the returned values.

Example:

```
# snmpwalk -Cp -On -c public -v1 10.20.30.29
.1.3.6.1.4.1.674.10892.1.700.20.1.8


.1.3.6.1.4.1.674.10892.1.700.20.1.8.1.1 = STRING: "ESM Frt I/
O Temp"
.1.3.6.1.4.1.674.10892.1.700.20.1.8.1.2 = STRING: "ESM CPU 1
Temp"
.1.3.6.1.4.1.674.10892.1.700.20.1.8.1.3 = STRING: "ESM CPU 2
Temp"
.1.3.6.1.4.1.674.10892.1.700.20.1.8.1.4 = STRING: "ESM Riser
Temp"
.1.3.6.1.4.1.674.10892.1.700.20.1.8.1.5 = STRING: "BP Bottom
Temp"
.1.3.6.1.4.1.674.10892.1.700.20.1.8.1.6 = STRING: "BP Top
Temp"
Variables found: 6
```

In this case, there are 6 temperature probes to monitor. You will have to add one task for each temperature probe you would like to monitor. The indices from this example are “1.1”, “1.2”, “1.3”, “1.4”, “1.5”, and “1.6”.

To configure this service to monitor the first temperature probe, enter “1.1” as the Temperature Probe Location Name Index, or enter "ESM Frt I/O Temp" as the Temperature Probe Location Name Value.

Status Details

Server Temp (Dell) Status Details

Status Detail	Description
Server Temp (Dell) Status	The probe status of the temperature probe. The possible states defined in the MIB are: • Other(1) • Unknown(2) • Ok(3) • nonCriticalUpper(4) • criticalUpper(5) • nonRecoverableUpper(6) • nonCriticalLower(7) • criticalLower(8) • nonRecoverableLower(9) • Failed(10) • 5,6,8-10 map to Failed in N-central, • 3 maps to Normal in N-central, and • anything else that maps to Warning.
Server Temp (Dell) Reading	The reading of the temperature probe. The value is an integer representing temperature, in degrees Centigrade.

Server Temp (HP)

Service Type: Network

Collection Method: SNMP

Instances on a Device: Single

Supported Platforms: Compaq/HP ProLiant Series Servers running Compaq Insight Manager v7

Device Class: Generic Server, Other, Printer, Scanner/Camera, Switch/Router, and Windows Server

Monitored By: Hardware Probe, Windows Probes

Service Version: N-central 5.0 and greater

The Server Temp (HP) service monitors the overall condition of the system’s thermal environment for Compaq/HP ProLiant servers.

Service Details

Server Temp (HP) Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	

Status Details

Server Temp (HP) Status Details

Status Details	Description
Server Temp (HP)	This value specifies the overall condition of the system's thermal environment: • Other(1), • Ok(2), • Degraded(3), and • Failed(4). In N-central, • 1 and 2 map to Normal, • 3 maps to Warning, and • 4 maps to Failed.

Chapter 69
SMTP

Service Type:	Network
Collection Method:	TCP
Instances on a Device:	Single
Supported Platforms:	N/A
Device Class:	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server
Service Version:	N-central 3.0 and greater

The Simple Mail Transfer Protocol (SMTP) test monitors the status of the SMTP process on a network device. SMTP is the standard Internet host-to-host email transport protocol. Typically, you use SMTP to send your email to a POP3 server, from where the recipient retrieves the message.

N-central can determine the up or down status of the SMTP service. The SMTP service does not use the Warning state. N-central averages the availability of the SMTP service over the scan interval. It compares the availability of the SMTP service to the threshold to determine the status.

Service Details

SMTP Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Timeout Value	
Port Number	
Validating String	

SMTP Status Details

Status Detail	Description
SMTP Service Availability	N-central determines whether the SMTP service is up or down. The SMTP service does not use the Warning state. N-central averages the availability of the SMTP service over the scan interval and compares the availability of the SMTP service to the threshold to determine the status.
Round Trip Time (ms)	The time (in milliseconds) for a request to be sent and received.
DNS Resolution	The threshold that determines whether the device name can be resolved. If an FQDN has been specified, the service searches for its IP address. If the IP address is found, the state will be Normal. Otherwise, it will be Failed, based on the default settings. If an IP address has been specified, the service checks only the IP address's format. If the format is correct, the state will be Normal. Otherwise, it will be Failed, based on the default settings.

Chapter 70

SMTP Queues

Service Type:	System
Collection Method:	WMI Server
Instances on a Device:	Single
Supported Platforms:	Any WMI-enabled Windows server that has an SMTP service running which reports data through the Win32_PerfRawData_SMTPServer class; for example, Microsoft Exchange
Device Class:	Windows Server
Monitored By:	Windows Probes
Service Version:	N-central 5.0 and greater

Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* published by Microsoft®.

The SMTP Queues service monitors the performance of the SMTP Server based on metrics obtained from the following properties:

- the remote queue length,
- the local queue length,
- the current inbound connections,
- the current outbound connections.

Service Details

SMTP Queues Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	
SMTP Service Name	An instance of the class Win32_PerfRawData_SMTPSvc_SMTPServe; for example, “SMTP1”.

Configuring SMTP Service Name

Use the Web Based Enterprise Management (wbemtest) tool in Windows to get the service name to enter in the setup.

To configure SMTP Service Name

1. Press the Windows Explorer key + R.
   ↳ The Run dialog box appears.
2. Specify wbemtest in the Open field, and press Enter.
   ↳ The Windows Management Instrumentation Tester dialog box appears.
3. Click Connect.
   ↳ The Connect dialog box appears.
4. In the first field, specify the namespace: \\<your host name>\root\cimv2.
5. Click Connect.
   ↳ The Windows Management Instrumentation Tester dialog box appears, with the namespace you have specified.
6. Click Enum Instances.
   ↳ The Class Info dialog box appears.
7. In the Enter superclass name field, specify: Win32_PerfRawData_SMTPSvc_SMTPServer.
8. Click OK.
   ↳ The Query Results dialog box appears, listing SMTP instances.
9. Enter an instance name from the list exactly as it is displayed, preserving the case and the spaces, in the SMTP Service Name field in the task properties under Setup>Devices on the central server.

Status Details

SMTP Queues Status Details

Status Detail	Description
Number of messages in the remote queue	See Status Detail.
Number of messages in the local queue	See Status Detail.
Number of connections currently inbound	See Status Detail.
Number of connections currently outbound	See Status Detail.

Chapter 71
SNMP

Service Type:	Network
Collection Method:	SNMP
Instances on a Device:	Single
Supported Platforms:	N/A
Device Class:	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, and Windows Workstation
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe
Service Version:	N-central 3.5 and greater

SNMP is a widely used network management protocol that is present in a majority of network infrastructures (routers, switches, firewalls, etc.) as well as in different types of computing platforms.

N-central can monitor values of counters and gauges associated with the use of SNMP within a network. These values indicate the general status of the SNMP agents running on the target devices.

Some of these counters may indicate attempts to exploit vulnerabilities in the SNMP protocol by external systems. Because these vulnerabilities have been well documented by the CERT Coordination Center (see Warning note below), many systems have been updated to correct problems that once existed. However, monitoring counters such as an Invalid Community String or an Invalid Operation can indicate if undesired SNMP traffic is being transmitted to the customer's network.

Warning! For information about SNMP security risks, see: http://www.cert.org/advisories/CA-2002-03.html. In addition, you should access the SNMP vendor's Web site for the latest updates, patches, and information about vendor-specific issues.

The table SNMPV2-MIB describes the SNMP objects that are queried by the probe.

SNMPV2-MIB

Object Descriptors	Numerical OID
snmpInBadVersions	1.3.6.1.2.1.11.3
snmpInBadCommunityNames	1.3.6.1.2.1.11.4
snmpInBadCommunityUses	1.3.6.1.2.1.11.5
snmpInASNParseErrs	1.3.6.1.2.1.11.6

Object Descriptors	Numerical OID
snmpInTooBigs	1.3.6.1.2.1.11.8
snmpInNoSuchNames	1.3.6.1.2.1.11.9
snmpInBadValues	1.3.6.1.2.1.11.10
snmpInGenErrors	1.3.6.1.2.1.11.12
snmpOutTooBigs	1.3.6.1.2.1.11.20

Service Details

SNMP Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	

Status Details

SNMP Status Details

Status Detail	Description
Number of SNMP messages with version error	The number of SNMP messages received by the SNMP agent on the target device that were for a version of SNMP that is not supported by the target device.
Number of wrong community string messages	The number of SNMP Messages received by the SNMP agent on the device that used an incorrect SNMP community string.
Number of messages with an invalid user	The number of SNMP Messages received by the SNMP agent on the target device which requested an SNMP operation which was not allowed by the SNMP community string in the Message.
Number of SNMP messages unparsed	The number of SNMP messages received by the SNMP agent on the target device with syntax errors.
Number of messages with invalid status bits	The number of SNMP messages received by or transmitted from the SNMP agent on the target device, which indicates an error status.

Chapter 72

SQL Server

Service Type: System

Collection Method: WMI Workstation

Instances on a Device: Multiple

Supported Platforms: Microsoft® SQL Server

Device Class: Windows Server and Windows Workstation

Monitored By: Network Windows Probe, Workgroup Windows Probe, WSP

Service Version: N-central 4.0 and greater

Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* published by Microsoft®.

The SQL Server service monitors the database files of the Microsoft® SQL server, including individual database instances and the sum of all of the specified instances of the SQL server.

During the monitoring process, the SQL Server service uses the Windows probe to measure the SQL server's key activities. The results are then displayed on the status dashboard for the service.

Service Details

SQL Server Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
WMI class name of Database Performance Counter	The name of the WMI class of the Database Performance Counter that is to be monitored.

Service Detail	Description
Instance Name	The instance name of the class that is specified in the WMI class name of Database Performance Counter. The instance will be monitored for active transactions, log file size (KB), data file size (KB), and the number of transactions occurred per second.
WMI class name of Server General Statistics Performance Counter	The name of the WMI class server general statistics performance counter that is to be monitored.
WMI class name of Server Lock Performance Counter	The name of the WMI class of the server lock performance counter that is to be monitored.
Instance Name	The instance name that is applied to the class names specified in WMI class name of server lock performance counter. The instance will be monitored for the average wait time and number of deadlocks occurred per second.

Status Details

SQL Server Status Details

Status Detail	Description
Active transactions	The threshold values that determine the status change of the service.
Log file size (KB)	
Data file size (KB)	
Transactions/second	
Number of user connections	
Average waiting time (ms)	
Deadlocks/second	

Chapter 73
SSH

Service Type: Network

Collection Method: TCP

Instances on a Device: Single

Supported Platforms: N/A

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server

Service Version: N-central 3.0 and greater

N-central can monitor the availability of a Secure Shell (SSH) daemon on a network device. SSH is a shell program for logging into and executing commands on a remote computer. It provides strong authentication and secure communications over a vulnerable connection. It also provides a UNIX shell augmented with a range of cryptographic options.

N-central can determine the up or down status of the SSH service. The SSH service does not use the Warning state. N-central averages the availability of the SSH service over the scan interval. It compares the availability of the SSH service to the threshold to determine the status.

Service Details

SSH Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Timeout Value	
Port Number	
Validating String	

Status Details

SSH Status Details

Status Detail	Description
SSH Service Availability	N-central determines whether the SSH service is up or down. The SSH service does not use the Warning state. N-central averages the availability of the SSH service over the scan interval and compares the availability of the SSH service to the threshold to determine the status.
Round Trip Time (ms)	The time (in milliseconds) for a request to be sent and received.
DNS Resolution	The threshold that determines whether the device name can be resolved. If an FQDN has been specified, the service searches for its IP address. If the IP address is found, the state will be Normal. Otherwise, it will be Failed, based on the default settings. If an IP address has been specified, the service checks only the IP address's format. If the format is correct, the state will be Normal. Otherwise, it will be Failed, based on the default settings.

Chapter 74

System Change

Service Type:	System
Collection Method:	System
Instances on a Device:	Single
Supported Platforms:	Microsoft® Windows®
Device Class:	Windows Server and Windows Workstation
Monitored By:	Central Server Asset
Service Version:	N-central 4.5 and greater

Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* published by Microsoft®.

The System Change service monitors the hardware components that have been discovered on a Windows device. Once these components have been discovered, N-central creates a snapshot of this asset information. This snapshot is then used by the System Change service as a baseline to monitor any changes that occur in the assets of the device. The service scans the device for changes every day at 9:00 a.m. For example, the removal of a network adapter at 1:00 p.m. is reflected in the state of the service at 9:00 a.m. the next day. This change is also reflected in the updated snapshot, which can then be reset as the new baseline. For more information about resetting the baseline, refer to Setting the System Change Baseline in the *Customer Manual*.

The System Change service requires the following configurations:

- The service can only be monitored on discovered assets, not on devices that have been manually created.
- The service needs to have a recurring Windows Asset Discovery task targeted against the IP address of the target device.
- The data presented in the service is collected by a Network - Windows or Workgroup - Windows probe. You must either install a Windows probe at the customer’s location or ensure a probe is installed that can access the target device through WMI.

Service Details

System Change Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	

Status Details

System Change Status Details

Status Detail	Description
Change in number of network adapters	The change in the number of assets. The number can reflect any addition or removal of assets. Information about the changes that have occurred in the asset details. Information about the changes that have occurred to the asset. The Stale state is displayed when a device's MAC address changes due to changes in its network adapter.
Change in network adapter details	
Change in number of CPUs	
Change in CPU details	
Change in number of media access devices	
Change in media access device details	
Change in number of video controllers	
Change in video controller details	
Change in size of RAM	
Change in OS	

Chapter 75

System Check-In

Service Type: System

Collection Method: Central Server Asset

Instances on a Device: Single

Supported Platforms: N/A

Device Class: Generic Server, Generic Workstation, Windows Server, and Windows Workstation

Monitored By: Central Server Asset

Service Version: N-central 5.0 and greater

The System Check-In service monitors roaming devices, such as laptops, to ensure their presence on the network. Their presence is determined by the frequency at which they connect to the network. For an accurate state to be determined, the device must remain connected to the network for the specified scan interval time.

When System Check-in is first added to a device, the service will be in a Misconfigured state until the device's agent first makes contact with the central server.

During the monitoring process, the central server queries the time of the most recent connection of a device's agent to the network. This is compared to the current time and the resulting difference is then compared to the specified threshold values so that it can be represented by the appropriate state on the status dashboard for the service.

Example: If the time difference between the previous and current connection is within 10 days, the service state will display Normal; between 10 and 15 days, Warning; and over 15 days, Failed.

Service Details

System Check-In Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Service Description	
Scan Interval	

Status Details

System Check-In Status Details

Status Detail	Description
System Check-In	The threshold that compares the time difference between the current time and the most recent connection to the specified threshold values.

Chapter 76

System Replacement

Service Type: System

Collection Method: Central Server Asset

Instances on a Device: Single

Supported Platforms: N/A

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Central Server Asset

Service Version: N-central 5.0 and greater

The System Replacement service monitors a device's expected replacement date, which can be specified when adding or editing the device. This service allows you to better monitor the life cycle of a device and avoid issues, such as excessive maintenance and support costs, and the inadequate total cost of ownership (TCO) data for purchase planning.

Service Details

System Replacement Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Service Description	
Scan Interval	

Status Details

System Replacement Status Details

Status Detail	Description
System Replacement	The threshold that determines when the device is to be replaced.

Chapter 77

System Warranty

Service Type: System

Collection Method: Central Server Asset

Instances on a Device: Single

Supported Platforms: N/A

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Central Server Asset

Service Version: N-central 5.0 and greater

The System Warranty service monitors a device's expected warranty expiry date, which can be specified when adding or editing the device. This service allows you to avoid issues, such as leasing penalties, additional buying costs, and the inadequate total cost of ownership (TCO) data for purchase planning.

Service Details

System Warranty Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Current Monitoring Probe	
Service Description	
Scan Interval	

Status Details

System Warranty Status Details

Status Details	Description
System Warranty	The threshold for expiry of the warranty.

Chapter 78

Telnet

Service Type:	Network
Collection Method:	TCP
Instances on a Device:	Single
Supported Platforms:	N/A
Device Class:	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server
Service Version:	N-central 3.0 and greater

The Terminal Network Protocol (Telnet) test checks the status of the telnet port on the network device. The Telnet protocol is designed for terminal-oriented remote login sessions.

N-central can determine the up or down status of the Telnet service. The Telnet service does not use the Warning state. N-central averages the availability of the Telnet service over the scan interval. It compares the availability of the Telnet service to the threshold to determine the status.

Service Details

Telnet Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Timeout Value	
Port Number	

Status Details

Telnet Status Details

Status Detail	Description
Telnet Service Availability	N-central determines whether the Telnet service is up or down. The Telnet service does not use the Warning state. N-central averages the availability of the Telnet service over the scan interval and compares the availability of the Telnet service to the threshold to determine the status.
Round Trip Time (ms)	The time (in milliseconds) for a request to be sent and received.
DNS Resolution	The threshold that determines whether the device name can be resolved. If an FQDN has been specified, the service searches for its IP address. If the IP address is found, the state will be Normal. Otherwise, it will be Failed, based on the default settings. If an IP address has been specified, the service checks only the IP address's format. If the format is correct, the state will be Normal. Otherwise, it will be Failed, based on the default settings.

Chapter 79

Terminal Server

Service Type:	System
Collection Method:	WMI Server
Instances on a Device:	Single
Supported Platforms:	Microsoft® Windows® Terminal Services
Device Class:	Windows Server
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server
Service Version:	N-central 4.0 and greater

Note: For devices running Windows XP SP2, you must enable the Windows Firewall: Allow remote administration exception setting before N-central can access and monitor devices using Windows Management Instrumentation. You will find the settings for the Windows Firewall in the Windows XP SP2 Control Panel. For more information, refer to *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* published by Microsoft®.

The Terminal Server service monitors the availability of the Microsoft Windows Terminal Services, which allows remote login to a server using the Microsoft Remote Desktop client.

During the monitoring process, the Terminal Server service uses the Windows probe to track the terminal server's key activities. The results are then displayed on the status dashboard for the service.

Service Details

Terminal Server Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	

Status Details

Terminal Server Status Details

Threshold	Description
Active sessions	Counts the sessions that are currently connected and have users logged on.
Inactive sessions	Counts the sessions that are: • Waiting for the initial connection; • Both, connected and waiting for users to log on; or • Both, disconnected and on which a user is logged on. For more information, refer to the table below, Table .
Total sessions	The sum of the active and inactive sessions.

Examples of Active and Inactive Session Counts

Example	Session Count
Terminal Server Shutting Down	Active Session Count = 0 Inactive Session Count = 0 Total Sessions = 0
Terminal Server Freshly Started	Active Session Count = 0 Inactive Session Count = 1 Total Sessions = 1
Session Connected But Not Logged On	Active Session Count = 0 Inactive Session Count = 2 Total Sessions = 2
Session Connected AND Logged On	Active Session Count = 1 Inactive Session Count = 1 Total Sessions = 2
Session Disconnected BUT Logged On	Active Session Count = 0 Inactive Session Count = 2 Total Sessions = 2

Chapter 80
Traffic

Service Type:	Network
Collection Method:	SNMP
Instances on a Device:	Multiple
Supported Platforms:	N/A
Device Class:	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Monitored By:	Network Hardware Probe
Service Version:	N-central 3.0 and greater

The Traffic service uses the Network Hardware probe to monitor the amount of data transmitted to and from network interfaces, such as switches and routers that access a particular device. The results from monitoring are displayed on the status dashboard under the Traffic service and, if specified, can also be provided in any notifications triggered by the service.

During the monitoring process, the probe sends an SNMP get request for values on the MIB objects that reside on a network interface. These values are used by the probe to calculate the network interface's utilization.

To monitor the Traffic service on a device, you must:

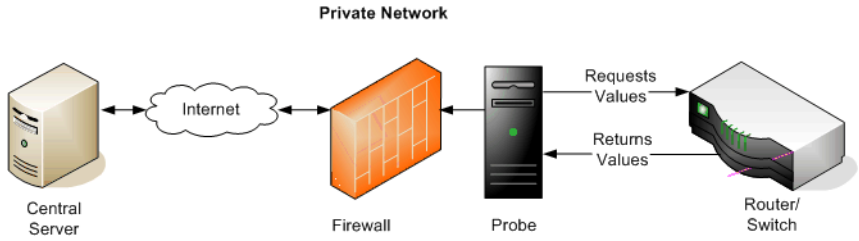
- Select the SNMP Enabled option when adding the device. For more information, refer to Adding Devices in the *Customer Manual*.
- Run interface discovery on the device. For more information, refer to Discovering Interfaces for SNMP Services in the *Customer Manual*.
- Add the Traffic service to the device. For more information, refer to Adding Services in the *Customer Manual*.
- set the Interfaces to Monitor service detail for the Traffic service. For more information, refer to Setting Interfaces for SNMP Services in the *Customer Manual*.

The table below describes the SNMP objects that are queried and Figure 80-1 describes the monitoring process, where the probe sends its calculations to the central server through the firewall.

IF-MIB

Object Descriptors	Numerical OID
sysUpTime	1.3.6.1.2.1.1.3
ifDescr	1.3.6.1.2.1.2.2.1.2
ifSpeed	1.3.6.1.2.1.2.2.1.5
ifInOctets	1.3.6.1.2.1.2.2.1.10
ifOutOctets	1.3.6.1.2.1.2.2.1.16

Figure 80-1: Monitoring Traffic



If the probe receives all of the values, it can calculate the traffic utilization. If the probe cannot receive values from one or more objects, it will send an error message to the central server and the state of the service will change to Misconfigured.

For example, the probe can calculate the outgoing bytes per second. If 43,950,073 bytes were transmitted to an interface at the time 00:05 and 43,988,841 bytes were transmitted to the same interface at the time 00:10, the outgoing bytes per second would be:

$$\frac{\text{43,988,841 bytes—43,950,073 bytes}}{\text{10 seconds—05 seconds}} = 7753 \text{ bytes/second}$$

The results of the calculations are evaluated against threshold settings, which in turn cause state changes for the device.

In N-central, the switch or router on which traffic is being calculated needs to be added as a device, and the Traffic service then needs to be added to the device before monitoring can begin.

Service Details

Traffic Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Interfaces to Monitor	The descriptions of the discovered interfaces.
Scan Interval	Refer to Table 1-1 on page 2.

Status Details

Traffic Status Details

Status Detail	Description
Thresholds	Determines the traffic saturation by comparing the monitored data to the threshold values.
Total bytes per second	The total bytes per second transmitted and received since the device was powered on.
Incoming bytes per second	The total bytes per second received since the device was powered on.
Outgoing bytes per second	The total bytes per second transmitted since the device was powered on.
Traffic Utilization (%)	The total bytes transmitted and received since the device was powered on as a percentage of the capacity.

Chapter 81
Veritas

Service Type:	System
Collection Method:	Log Appended
Instances on a Device:	Single
Supported Platforms:	Veritas™ Backup Exec™, up to version 10
Device Class:	Generic Server, Generic Workstation, Windows Server, and Windows Workstation
Monitored By:	Agent (Windows)
Service Version:	N-central 3.0 and greater

N-central monitors the completion of a backup that is performed with the Veritas™ Backup Exec™ software. It determines the success or failure of a Veritas backup by locating and reviewing the log files generated by the backup software. For Veritas 9 and 10, although several log file formats exist, N-central processes only specific log file formats.

Veritas 9 and 10 are supported only by Microsoft Windows® agents. It further supports the ASCII code and unicode and the XML format of the Veritas log file.

At run time, the agent scans the Veritas logs. At this specified time and frequency, the agent checks if the log file directory exists. If the directory does not exist, the agent reports the Failed state to the central server. If the directory exists, the agent searches for the log files with the specified prefix and suffix; it opens the most recently modified file and compares the start time of the backup cycle and to the current time of its machine.

If the difference between the start time and the current time is greater than the specified time offset, the log file is considered old and the agent reports the Failed state to the central server.

If the difference between the start time and the current time is equal to or less than the specified time offset, the agent performs tasks based on the version of the Veritas backup software:

- For Veritas versions 8 and lower, the agent checks the log file for the specified keyword. If it finds the keyword, it will report the Failed state to the central server. If it does not find the keyword, it will report the Normal state to the central server.
- For Veritas versions 9 and 10, the agent looks for system-specified status codes in the xml log file. If these status codes match specified job status values, the agent displays the Failed status on the status dashboard. If the agent does not find a match, it displays the Normal state to the central server.

The central server will not consider the data from the Veritas service to be stale until 24 hours have passed since the last time it reported to the central server.

The Veritas service supports wide characters.

Service Details

Veritas Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Service Description	
Keyword	The keyword: • is case-sensitive, • can contain punctuation, • cannot use wildcards, • can contain spaces, and • only supports version 8 and lower versions of Veritas. You must omit unwanted trailing spaces. For example, if the keyword is defined as “Fail” (with no spaces) and Veritas backed up a file called “C:\My Documents\Devices\DevicesThatFailed.doc”, the agent reports a backup failure to the server. However, if the failure string was defined as “Fail ” (with a space before and after the word Fail), the same file would not cause a false Failed state. The agent opens the log file with the newest timestamp. If the keyword appears anywhere in the log file, the Veritas service transitions to the Failed state.
Log File Prefix Log File Suffix	If you use the defaults, the agent selects all of the files matching bex*.txt for consideration. For example, if you change the prefix and suffix to “veritas” and “log.txt”, the agent selects all of the files matching veritas*log.txt for consideration. The log file prefix and suffix are strings used to find log files within the log file directory. If the log file directory exists, the agent strips the prefix and suffix from the file names and looks for the file with the newest timestamp. The prefix and suffix cannot contain spaces or use wildcards. The suffix must include the period. If the agent cannot find a file with the specified prefix and suffix, it reports the Failed state to the central server. If the log file has a .xml suffix, then N-central processes this file as a Veritas 9 or 10 file. The suffix for Veritas 9 and 10 is not case-sensitive.

Service Detail	Description
Log File Directory	The log file directory is a full path and can contain spaces. The trailing backslash is required. For example: C:\Program Files\Veritas\Logs\ The directory in which to search for log files. At run time, the agent checks that the log file directory exists. If the directory does not exist, the Veritas service transitions to the Failed state.
Time Offset	Refer to Table 1-1 on page 2.
Start Time	
End Time	
Scan Interval	
Repeat Weekly on Day(s)	
Repeat Monthly on Day(s)	

Status Details

Veritas Status Details

Status Detail	Description
Veritas Service Availability	N-central determines the quality of performance by comparing the monitored data to the thresholds. The availability range is 0-255, which corresponds to the following: Normal = 1, Warning = 2-255, and Failed = 0.
Backup duration (Seconds)	The thresholds to track the progress of a backup.
Data amount backed up (Bytes)	The thresholds to track the number of bytes that are backed up. For example, backup tapes have a fixed size, and this threshold can ensure that the backup size does not exceed the space on the backup tape. Also, this threshold can help you track significant changes in the size of a backup file. For example, if the backup file is usually 75GB in size, and the backup result displayed 5GB, then this can indicate a loss of data in the backup file.
Job Status for Veritas 9 and 10	Refer to Job Status for Veritas 9 and 10 on page 253
Veritas Service Details	Describes the results of the latest scan. For example: Job start time is beyond the offset, this log file c:\Program Files\Veritas\Backup Exec\Nt\Data\BEX01586.xml is an old log file

Job Status for Veritas 9 and 10

You can view the return values for the associated job status on the status screen for the Veritas service. These values represent specific critical issues. They are returned by Veritas Backup Exec and reported by the agent. For the return values: 1, 5, 6, 7, 8, 9, 10, 11, 12, 14, 16, 20, 21, 22, and 23, the agent reports the Failed state to the central server. For the value 3, the agent reports the Warning state.

The table Return Values of Veritas 9 and 10 Job Statuses and Critical Issues describes the job statuses and critical issues associated with the return values that are monitored by Veritas Backup Exec 9 and 10.

Return Values of Veritas 9 and 10 Job Statuses and Critical Issues

Return Value	Job Status	Description of Critical Issue
1	Cancelled	Job is terminal due to cancellation.
2	Completed	Job has been completed by the engine and is waiting final disposition.
3	Successful with exceptions	Job is terminal with success but there are some exceptions.
4	Dispatched	Job has been sent for execution.
5	Hold	Job is in a hold state.
6	Error	Job is terminal with an error.
7	Invalid schedule	The schedule for the task is invalid.
8	Invalid time window	The time window is mutually exclusive thus job will never run.
9	Missed	Job is eligible for dispatch and is late.
10	Not in window	Date of job makes it eligible to run, but time is not in window.
11	Ready but paused	Job is ready, but dispatcher is paused.
12	Pending	The job needs to be dispositioned to an actual state.
13	Recovered	The system forced recovery of the job.
14	Disabled	Job has been disabled in the system.
15	Resumed	The job will be restarted with check point restart enabled, this value is only set in the job history summary.
16	Active	Job is currently running on server.
17	Ready	Job is eligible for dispatch.
18	Scheduled	The job has a due date in the future.
19	Success	Job is terminal with success.
20	Superseded	Job is ready, but another higher precedence task is eligible to run.
21	Threshold auto-abort	The job was aborted due to Abort Threshold time-out.
22	To be scheduled	The job needs to have the due date calculated.
23	Linked job	The job is linked to another job so will not start until the master job is finished.

Chapter 82
VNC

Service Type:	Network
Collection Method:	TCP
Instances on a Device:	Single
Supported Platforms:	N/A
Device Class:	Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server
Service Version:	N-central 3.0 and greater

N-central can monitor the availability of a Virtual Network Computing (VNC) server.

N-central can determine the up or down status of the VNC service. The VNC service does not use the Warning state.

N-central averages the availability of the VNC service over the scan interval. It compares the availability of the VNC service to the threshold to determine the status.

Service Details

VNC Service Details

Service Details	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Timeout Value	
Port Number	
Validation String	

VNC Status Details

VNC Status Details

Status Detail	Description
VNC Service Availability	N-central determines whether the VNC service is up or down. The VNC service does not use the Warning state. N-central averages the availability of the VNC service over the scan interval and compares the availability of the VNC service to the threshold to determine the status.

Chapter 83

Windows Terminal Server

Service Type: Network

Collection Method: Generic TCP

Instances on a Device: Multiple (up to 3 instances)

Supported Platforms: Microsoft® Terminal Services

Device Class: Generic Server, Generic Workstation, Other, Printer, Scanner/Camera, Switch/Router, Windows Server, and Windows Workstation

Monitored By: Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server

Service Version: N-central 4.5 and greater

The Windows Terminal Server service monitors the availability of the port, which the clients of the Microsoft Terminal Services use to connect to the Terminal Services application. The availability of the port, which is determined by the service testing the port's connectivity, indicates that the Terminal Services are able to connect to the Terminal Services application. This service also measures the domain name system (DNS) resolution and the round trip time of the initial connection request and response. The availability results of the TCP service are then reflected on the status dashboard for the Windows Terminal Server service.

A maximum of three instances of this service can be set on a device, with each instance monitoring a different port on the device.

The Windows Terminal Server service does not use the Warning state.

Service Details

Table 83-1: Windows Terminal Server Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time to Stale	
Monitoring Probe	
Service Description	
Scan Interval	
Timeout Value	
Port Number	

Status Details

Table 83-2: Windows Terminal Server Status Details

Threshold	Description
Terminal Services (TCP) Availability	The threshold that determines the availability of the port.
Round Trip Time (ms)	The time (in milliseconds) for a request to be sent and received.
DNS Resolution	The threshold that determines whether the device name can be resolved. If an FQDN has been specified, the service searches for its IP address. If the IP address is found, the state will be Normal. Otherwise, it will be Failed, based on the default settings. If an IP address has been specified, the service checks only the IP address's format. If the format is correct, the state will be Normal. Otherwise, it will be Failed, based on the default settings.

Chapter 84
WTS

Service Type: Network

Collection Method: HTTP

Instances on a Device: Multiple

Supported Platforms: N/A

Device Class: Generic Server, Other, Printer, Scanner/Camera, Switch/Router, and Windows Server

Monitored By: Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server

Service Version: N-central 5.0 and greater

The Web Transaction Service (WTS) monitors the specific content on a Web site by searching for a matching regular expression. For example, you can monitor the availability of specific content on an e-commerce site that uses a database-driven architecture.

The results from monitoring are displayed on the status dashboard under the WTS service. If specified, the results can also be provided in any notifications triggered by the service.

The WTS uses HTTP for monitoring. For more information about HTTP, refer to HTTP on page 147.

Service Details

Table 84-1: Web Transaction Service Details

Service Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	
Timeout Value	
Port Number	
Validating String	

Service Detail	Description
HTTP URL	The URL used to test the availability of the Web server. For example: • www.xyz.com, index.html, • http://www.xyz.com/index.html, or • http://www.xyz.com/ A partial URL is accessed using the network routable address of the Web server.
Normal Response Code	The codes in the response header that indicate a Normal state.
Warning Response Code	The codes in the response header that indicate a Warning state.
Content Verification Regular Expression	The regular expression used to find a specific match in the content on the Web page. For example: The page cannot be displayed.

Status Details

Table 84-2: Web Transaction Service Status Details

Status Details	Description
WTS Service Availability	The availability of the port.
Average Round Trip Time (ms)	The average time (in milliseconds) for a request to be sent and received.
DNS Resolution	The FQDN or IP address that determines whether the device name can be resolved. If an FQDN has been specified, the service searches for its IP address. If the IP address is found, the state will be Normal. Otherwise, it will be Failed, based on the default settings. If an IP address has been specified, the service checks only the IP address' format. If the format is correct, the state will be Normal. Otherwise, it will be Failed, based on the default settings.
Content verification regular expression	The regular expression that triggers the status for the matched contents on the Web page.

Chapter 85
WTSS

Service Type:	Network
Collection Method:	HTTPS
Instances on a Device:	Multiple
Supported Platforms:	N/A
Device Class:	Generic Server, Other, Printer, Scanner/Camera, Switch/Router, and Windows Server
Monitored By:	Network Hardware Probe, Network Windows Probe, Workgroup Windows Probe, WSP, Central Server
Service Version:	N-central 5.0 and greater

The Web Transaction Service (S) (WTSS) monitors the specific content on a Web site over a secure Web connection by searching for a matching regular expression. For example, you can monitor the availability of specific content on an e-commerce site that uses a database-driven architecture.

The results from monitoring are displayed on the status dashboard under the WTSS service. If specified, the results can also be provided in any notifications triggered by the service.

The WTSS uses HTTPS for monitoring. For more information, refer to HTTPS on page 149.

Service Details

Table 85-1: Web Transaction Service (S) Details

Detail	Description
Monitoring	Refer to Table 1-1 on page 2.
Time To Stale	
Current Monitoring Probe	
Change Monitoring Probe	
Service Description	
Scan Interval	
Timeout Value	
Port Number	
Validating String	

Detail	Description
HTTP URL	The URL used to test the availability of the Web server. For example: • www.xyz.com, index.html, • https://www.xyz.com/index.html, or • https://www.xyz.com/ A partial URL is accessed using the network routable address of the Web server.
Normal Response Code	The codes in the response header that indicate a Normal state.
Warning Response Code	The codes in the response header that indicate a Warning state.
Content Verification Regular Expression	The regular expression used to find a specific match in the content on the Web page. For example: The page cannot be displayed.

Status Details

Table 85-2: Web Transaction Service (S) Status Details

Status Details	Description
WTSS Availability	The availability of the Web server. If the CA certificate of the Web server has not been uploaded or is not listed in the default CA certificate file, this threshold will display Failed.
HTTPS Response Time	The time (in minutes) for the Web server to respond with the specified Web page.
DNS Resolution	The FQDN or IP address that determines whether the device name can be resolved. If an FQDN has been specified, the service searches for its IP address. If the IP address is found, the state will be Normal. Otherwise, it will be Failed, based on the default settings. If an IP address has been specified, the service checks only the IP address' format. If the format is correct, the state will be Normal. Otherwise, it will be Failed, based on the default settings.
Server Certificate Signature	The test that validates the encrypted signature of the SSL certificate.
Server Certificate Expiration (days)	The number of days remaining before the expiration of the SSL certificate.
Content verification regular expression	The regular expression that triggers the status for the matched contents on the Web page.

Index